Michigan Journal of Race and Law

Volume 11

2006

Constitutional Cash: Are Banks Guilty of Racial Profiling in Implementing the United States Patriot Act?

Cheryl R. Lee
Western State University College of Law

CONSTITUTIONAL CASH: ARE BANKS GUILTY OF RACIAL PROFILING IN IMPLEMENTING THE UNITED STATES PATRIOT ACT?

*Cheryl R. Lee**

History teaches us that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure.[1]

INTRODUCTION

If you are Black or Brown and living in America, you have probably been stopped and questioned by the police at some moment in your life. Since the passing of the Uniting and Strengthening America by Providing Appropriate Tools to Intercept and Obstruct Terrorism (hereinafter the USA Patriot Act), if you are Brown, Muslim, a foreign national of Middle

* Associate Professor of Law, Western State University College of Law; Northeastern University, B.S. 1982; Duquesne University School of Law, J.D. 1985. The author wishes to thank Professor Cliff Rectschaffen for his caring inspiration. Professor Lee also wishes to thank and congratulate her multi-talented teaching and research assistant Quiana Atkins-Canada, a 2005 L.L.M. Graduate in Intellectual Property at Golden Gate University School of Law.

1. Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 635 (1989) (Marshall, J., dissenting).

Eastern descent, "look Muslim" or "of Middle Eastern ethnicity," that questioning may happen in a bank.

Black people know if they try to hail a cab they may be assumed to be a threat or to be unable to pay. Or, if African Americans include certain upscale department stores in their shopping plans, they may be followed because of the presumption they are going to steal. Additionally, by now everyone in America knows that if you are Black and driving a luxury car on any highway in this country, you should be prepared to be stopped and questioned.[2]

For probably the first time in America, Blacks may not be the most suspicious people of color, at least not when terrorism is basis for suspicion. People of Middle Eastern descent are being arrested for minor visa defects, defects mostly attributed to Department of Homeland Security (DHS) administrative errors. Many of South Asian, Muslim, Arab, and even African descent have been victims of widespread FBI detentions, CIA and FBI interrogations, local police department roundups and unjustified arrests.[3] Since 9/11, Brown people, those of, or "appearing to be" of, Middle Eastern descent, know they may be assumed to be a threat in public crowds; in airports; on aircrafts, trains, buses; at automobile check points, and at national landmarks or urban buildings of significance. They know if they are traveling outside American borders, upon return to this country they *will be* presumed to be a threat of national significance. Many understand that if they walk into a bank to transact business, they are likely to be profiled, reported to the U.S. Treasury Department or scrutinized because of the presumption that they are terrorists or con-

---

2. DEBORAH RAMIREZ ET AL., A RESOURCE GUIDE ON RACIAL PROFILING DATA COLLECTION SYSTEMS, PROMISING PRACTICES AND LESSONS LEARNED 4 (2000), *available at* http://www.ncjrs.gov/pdffiles1/bja/184768.pdf. (confirming that most Americans, regardless of race, believe that racial profiling is a pervasive social problem and disapprove of the practice). Ramirez observes:

> National surveys have confirmed that most Americans, regardless of race, believe that racial profiling is a significant social problem. According to a Gallup Poll released on December 9, 1999, more than half of Americans polled believed that police actively engage in the practice of racial profiling and, more significantly, 81 percent of them said they disapprove of the practice. In a national sample of adults, 59 percent said that racial profiling is widespread. When the responses to the survey question were broken down by race, 56 percent of Whites and 77 percent of Blacks responded that racial profiling was pervasive. Additionally, the Gallup survey asked respondents how often they perceived having been stopped by the police based on their race alone. Six percent of Whites and 42 percent of Blacks responded that they had been stopped by the police because of their race, and 72 percent of Black men between ages 18 and 34 believed they had been stopped because of their race.

3. Arnoldo García, *No Nation of Immigrants Would Treat Immigrants This Way*, NETWORK NEWS (2002),*available at* www.nnirr.org/news/archived_netnews/no_nation.htm (describing the thousands of Arab, South Asian, Muslim, and Sikh immigrants illegally detained and made to submit to "voluntary" questioning and interviews since September 11, 2001).

nected to terrorist activity. At the very least, the response from bank personnel to their banking will be markedly different than that received prior to 9/11.

Incidents of hate crimes against *American* Muslims increased by 121% in 2003.[4] Being Muslim or "looking" Muslim or Middle Eastern can get your bank account closed, credit card cancelled, application or transaction at the bank branch office rejected, money wires refused, and business relationships may be scrutinized. All this can happen without your name being on, or in any way connected with, the Treasury Department's list of suspicious persons.[5] Does this sound like America during the McCarthy era, or during the Civil Rights Movement? This is what *American* citizens, Muslim, Middle Eastern or those who "look" Muslim or Middle Eastern, are facing in 2006.

Of course, racial profiling[6] is not new; it is embedded in the fabric of America. Profiling was born in the days of slavery when a slave could be killed unless they could produce on demand a "pass" when on the road to carry out master's business. Now, "[a]s it has done in the past, the FBI is once again targeting ethnic, political, and religious minority communities disproportionately ... with its surveillance and enforcement efforts .... a 'Special Registration' program now requires tens of thousands of Arab and Muslim immigrants to submit to a call-in interview from which other

---

4. Abdus Sattar Ghazali, *Hate Crimes Against American Muslims Up 121 Percent,* AM. MUSLIM PERSP., May 4, 2004, *available at* http://www.amp.ghazali.net/html/hate_crimes_report_html.

5. Using FINCEN (The Financial Crimes Enforcement Network), banks check names against several lists maintained by the Treasury Department, the State Department, the Department of Justice, the Federal Bureau of Investigations, the United Nations, the European Union, and entities in countries such as Canada and the United Kingdom. The lists include 390,000 names from 239 countries. The Financial Crimes Enforcement Network is the arm of the Treasury Department responsible for overseeing and implementing policies to prevent and detect money laundering in general and money laundering specifically related to terrorism.

6. Racial Profiling Data Collection Resource Center at Northeastern University, *Background and Current Data Collection Efforts: History of Racial Profiling Controversy* (Nov. 2000), *available at* http://www.racialprofilinganalysis.neu.edu/article:

> [A] profile is a coherent set of facts—known conditions and observed behavior—that indicate a particular individual may be engaged in criminal activity. Profiling first became associated with a method of intercepting drug traffickers during the 1970's. In 1985 Operation Pipeline instituted by the Drug Enforcement Administration (DEA) was designed as an intelligence-based assessment of the method by which drug networks transported bulk drugs to the marketplace, but became by virtue of the training of state police to be used as a drug courier profile on highways, a technique to target [B]lack and Hispanic male drivers by stopping them for technical traffic violations as a pretext for ascertaining whether they were carrying drugs.

immigrants are exempted."[7] Generally, hate crimes motivated by race in the past five years have increased.[8]

As with lynching in the 1800s and 1900s, the Civil Rights Movement, and the 1992 Rodney King beating, America continues this pattern of profiling. While profiling has always been institutional and government-sponsored, under the cover of "terrorism" it is now legitimately used by many more, from anyone in the tiniest local police agency to the National Security Service.

Government-condoned racial profiling increases the likelihood of private acts of racial profiling. The Civil Rights Movement gained momentum in response to police sanctioned segregation and profiling in America.

Take for example the following incidents:

1. In Corpus Christi, Texas, on July 14, 2004, George and Samimah Aziz-Hodge woke up to the image of a cross burned on the front lawn of their Country Club Estates home.[9]

2. In February 2004,—Muhammad Siddiqui, a Houston architect, husband to a busy physician and father of two young children, was home with his children, and received a visit from two FBI agent. He opened the door, and responded to their request to question him by saying, "I'd be happy to talk with you, but I'd like to have my attorney present." One of the agents told him he did not need an attorney, that would only make him look guilty. The agent insisted Siddiqui submit to the interview "now."[10]

---

7. *See* ANN BEESON & JAMEEL JAFFER, UNPATRIOTIC ACTS: THE FBI'S POWER TO RIFLE THROUGH YOUR RECORDS AND PERSONAL BELONGINGS WITHOUT TELLING YOU 8,9. (2003); Eric Lichtblau, *F.B.I Tells Offices to Count Local Muslims and Mosques,* N.Y. TIMES, Jan. 28, 2003, at A13 (reporting an F.B.I. order to field offices to count the number of Muslims and mosques in their districts in order to "establish a yardstick for the number of terrorism investigations and intelligence warrants"). *See also* AMERICAN CIVIL LIBERTIES UNION, FREEDOM UNDER FIRE: DISSENT IN POST 9/11 AMERICA (2003).

8. F.B.I. REPORT, TERRORISM 2000/2001, *available at* www.fbi.gov/publications/terror/terror2000_2001.pdf; F.B.I. REPORT, HATE CRIME STATISTICS 2003, *available at* http://www.FBI.gov/ucr/ucr.htm (reporting that 8,715 criminal offenses were identified as being motivated by hate, and that offenses based on race account for the highest category of hate crimes at 52.5%); The Human Rights Campaign, *Alarming Rates of Hate Crimes Reported By FBI* (2004), http://www.hrc.org/Content/ContentGroups/News_Releases/20042/Alarming_Rates_of_Hate_Crimes_Reported_by_FBI.htm (explaining that the reporting of these crimes is voluntary for local jurisdictions and hate crimes often go unreported by victims due to fear and stigmatization); William B. Rubenstein, *The Real Story of US Hate Crime Statistics: An Empirical Analysis,* 78 TUL. L. REV. 1213, 1229 (2004) (stating that Blacks report two thirds of 4600 racial hate crimes reported a year).

9. *Cross Burning Family Calls for National Investigation,* THE SAN DIEGO VOICE AND VIEWPOINT, July 29, 2004, at A1.

10. *See* Hamdi v. Rumsfeld, 316 F.3d. 450, 466 (4th Cir. 2003) (holding that if a person is designated as an enemy combatant, the executive administration obtains virtually

Siddiqui again asked to have his attorney present. The FBI agent responded angrily, prompting Siddiqui to call his attorney immediately. The attorney advised the agents that her client did not wish to speak with them at that time, but they could call her office and make an appointment to speak with him. The FBI agent responded by screaming at the attorney that Siddiqui did not have the right to counsel, an absolute misrepresentation of the law. The agent refused any further conversation with the attorney, instead shouting at Siddiqui to "turn off that cell phone!" One of the agents pulled back his coat to reveal a gun, scaring Siddiqui, whose children were still present. The incident ended when the agents realized they would not prevail and left, only after threatening Siddiqui. The next day, an FBI agent confirmed that Siddiqui was never a criminal target.[11]

3. In March 2004, the Equal Employment Opportunity Commission announced a $1.1 million settlement against Stockton Steel of California for workplace discrimination against Muslims. Four Pakistani machine operators had alleged they were routinely given the worst jobs, ridiculed during their daily prayers, and called "camel jockeys" and "ragheads." Similarly, in the fall of 2002, EEOC reached a $35,000 settlement with a North Carolina medical clinic that had ordered a Muslim nurse not to wear her religious headscarf. In January 2005, another EEOC suit was filed against Norwegian Hospital in Chicago for firing Ms. Abdullah, an employee whose family has lived in the U.S. for generations, for referring to Ramadan as "Taliban," and telling Ms. Abdullah she should leave the country if she did not like the way she was being treated.[12]

Discrimination against Muslims is clear; however, Americans are unfamiliar with this discrimination in banks. After the Great Depression, Americans in this country were re-taught to trust banks. Trusting banks is bred into our children. Washington Mutual Bank branch offices across this country conduct "school days" during which an officer of the bank

---

complete discretion over the length of detention and whether the detainee is entitled to consult a lawyer); Steve Fainaru & Dan Eggen, *Judge Grants "Combatant" Access to an Attorney*, WASH. POST, Dec. 5, 2002, at A1.

11. AMERICAN CIVIL LIBERTIES UNION, SANCTIONED BIAS: RACIAL PROFILING SINCE 9/11 15 (2004), *available at* http://www.aclu.org/FilesPDFs/racial%20profiling%20report.pdf.

12. Marjorie Valbron, *Career Journal: More Muslims Claim They Suffer Job Bias*, WALL ST. J., Apr. 15, 2003, at B1.

actually goes to the local elementary school to accept deposits from every child who wants to open or grow his own account.[13] Ordinarily, no American today would think a bank would discriminate against individuals because of their surname or how they look. But current bank behavior is demonstrative of something new.

President Clinton declared racial profiling a "morally indefensible, deeply corrosive practice," and further stated that "racial profiling is in fact the opposite of good police work, where actions are based on hard facts, not stereotypes. It is wrong, it is destructive, and it must stop."[14] Yet after the terrorist attack on the World Trade Center, the Pentagon, and in Pennsylvania, law enforcement began to disregard the traditional need to find probable cause before intruding into a citizen's personal affairs. In their zest to flush out the funds of foreign nationals who financed terrorism—the magnitude of which this country had never before seen[15]—the Fourth Amendment was trumped. The government's first response, in the name of national security, was to invade the privacy of citizens by using tools already in place. Racial profiling was immediately employed. Then, government agencies found they needed more latitude to legitimize their probes. Their answer? The USA Patriot Act. Patriot Act I is an attempt by the Treasury Department, the Department of Justice, the National Security Service and the Federal Bureau of Investigation to build a master list of "evil doers" and their possible activities. One goal? To try to determine where terrorist cash may be located in this country at any given moment.

If an individual conforms to the bank policy's defined profile, and attempts a perfectly legal monetary transaction—which has been designated by the bank as high risk, or is perceived to be suspicious, or a violation of any law or regulation—service will either be refused or a Suspicious Activity Report (SAR)[16] or Cash Transaction Report

---

13. Washington Mutual Bank, *School Savings*, http://www.wamu.com/personalbanking/newaccountschoices.

14. U.S. Department of Justice, Attorney General's Conference on Strengthening Police-Community Relationships, Report on the Proceedings, June 9–10, 1999, at 22–23.

15. *See* PETER SIGGINS, MARKKULA CENTER FOR APPLIED ETHICS, RACIAL PROFILING IN AN AGE OF TERRORISM (2002), http://www.scu.edu/ethics/publications/ethicalperspectives/profiling.html (explaining federal investigations of more than 5000 young Middle Eastern men from countries linked to terrorism which included contacting administrators at more than two hundred colleges and universities to obtain information about these young men).

16. 12 C.F.R. 208.20 (c)(2)(1995) (Suspicious Activity Reports, previously called Criminal Referral Forms). Hereinafter referred to in this article as "SARs," these forms were created by the Bank Secrecy Act & Annunzio-Wylie Anti-Money Laundering Act and are used by banks to report any suspicious transaction that may suggest money laundering, terrorist activity, or a customer that appears to be avoiding BSA reporting requirements to avoid the filing of a SAR or CTR. According to the BSA, a SAR must be filed if a bank has any reason to suspect that a transaction involves funds derived from illegal activity or is intended to disguise funds or assets derived from illegal activity; serves no apparent business or lawful purpose; or is designed to evade BSA regulations; and if the

(CTR)[17] (both created by the existing Bank Secrecy Act, also known as the Currency and Foreign Transactions Reporting Act)[18] will be generated and sent to the government.

This Article begins by comparing the concerns of American racial profiling to current terrorism concerns. Part II is an overview of the Bank Secrecy Act and its role in privacy issues concerning bank customers (as the predecessor to the USA Patriot Act). Here, the value of traditional reporting devices, specifically CTRs and SARs used by banks to alert law enforcement to possible terrorist activities, are discussed and evaluated. The facts suggest these reports have been ineffective in identifying terrorists, and have not only greatly infringed upon First Amendment[19] privacy rights, but also diminished the Fourth Amendment[20] protection against warrant-less searches of American bank account holders. Although the Supreme Court has previously ruled on the Constitutionality of these issues, I suggest that they must now reexamine a decision which many always felt was illogical, but has become increasingly so in today's fear-driven environment. Part III explores the policies banks initiated to comply with Patriot Act I, and the possibility that those policies have contributed, to the racial profiling of certain individuals of, or mistaken for, being of Middle Eastern descent. Part IV is an analysis of some of the problems Patriot Act I created. Part V highlights the dangers of The Proposed Domestic Security Enhancement Act, also known as Patriot Act II. Part VI discusses the desperate need to pass the End Racial Profiling Act (ERPA)[21] and evaluates whether the changes in bank policy attributed to Patriot Act I and proposed Patriot Act II are essential to the government's ability to strengthen national security and root out terrorists in our midst, even though they compromise the financial privacy Americans expect and believe in. Finally, the Conclusion proposes several solutions to protect American Constitutional liberties, obtain the intelligence necessary to protect us from terrorism, while most importantly beginning the process of repairing the psyche of America.

---

bank after examining the available facts knows of no reasonable explanation for the transaction, it must be reported).

17. 31 C.F.R. 103.22(a)(1)(2005) (requiring all financial institutions to file Cash Transaction Reports (CTRs) for each deposit, withdrawal, exchange of currency, payment and/or transfer to or by any bank involving a currency transaction or combination of transactions in the same business day involving more than $10,000 and the transportation of currency over $10,000 either into or out of the country).

18. Bank Secrecy Act (BSA), 12 U.S.C. §§ 1829(b), 1951–1959 (2000); 31 U.S.C. §§ 5311–5322 (2003).

19. *See* U.S. CONST. amend. I.

20. *See* U.S. CONST. amend. IV.

21. End Racial Profiling Act, H.R. 3847, 108th Cong. (2003); S. 2132, 108th Cong. (2003).

I. THE RACIAL PROFILING PROBLEM

"Amnesty International USA estimates that almost one in three people in the United States– approximately 87 million individuals in a total population of approximately 281 million– is at high risk of being subjected to some form of racial profiling."[22]

Admittedly, terrorism is an immeasurable threat to national security. But the terrorist-driven legislative impingement on American civil rights is of equal magnitude. Ethnic hatred, radical religious passion and nationalist zealousness, fused with terrorism, has caused centuries of human agony. Many of the attacks attributed to terrorism, in the United States and abroad, have been committed by people of Middle Eastern descent. However, this should not lead government officials to automatically conclude that because one is, or "appears to be" of, Middle Eastern descent, they are a security risk. This suspicion is especially troublesome when held by bank officials, in light of the suspiciousness with which minorities already view banking institutions. Certain American ethnic groups have spent decades trying to convince their Depression-era elderly, militant or simply conspiracy-theory happy relatives to take their money out of the jar buried in the backyard, or from under the mattress or in the sock drawer, and entrust it to a bank. If you are Brown, the fear your account may be in jeopardy touches you in each banking transaction or interaction with bank personnel. Is that fear legitimate? Absolutely. Patriot Act I puts banks in the business of practicing selective enforcement and racial profiling with every transaction, every hour of every business day. Fear of terrorism does not justify such suspicion.[23]

Maintaining that "the decisions regarding account closing are based on account activity, not on factors such as ethnicity, race, religion and country of origin," Fleet Boston Financial Corp closed 15 Muslim and Arab accounts without explanation.[24] Fleet has been a hotbed of suspicion

---

22. AMNESTY INTERNATIONAL USA, THREAT AND HUMILIATION, RACIAL PROFILING, DOMESTIC SECURITY, AND HUMAN RIGHTS IN THE UNITED STATES: THE HUMAN IMPACT OF RACIAL PROFILING 2 (2005).

23. The government maintains master lists of foreign banks, specially designated nationals and blocked persons, and suspected terrorists that banks use for guidance when considering whether a transaction or an individual should be the subject of a CTR or SAR. Current blocking profiles from the U.S. Department of Treasury, Office of Foreign Assets Control and Financial Crimes Enforcement Network, and U.S. Department of Justice Criminal Division, include individuals and entities appearing on OFAC's Specially Designated Nationals and Blocked Persons ("SDN") list: Cuban, North Korean, and Iranian citizens, wherever located; individuals living in North Korea, Iran or Cuba, regardless of citizenship; companies (including banks) located in North Korea, Cuba, areas of Bosnia and Herzegovina controlled by Bosnian Serb forces; those engaging in certain transactions with Angola; and governmental entities and officials of Libya, Iran, Iraq, and North Korea.

24. Matthew Brelis, *Muslim Society Presses Fleet Challenges Decision to Shut 15 Accounts with Arabic Names,* BOSTON GLOBE, Apr.4, 2003, at D1.

in the area of discrimination, paying more than $100 million in Georgia in 1996 to settle class actions over discrimination. In 1995, the Justice Department investigated the bank for allegedly charging minority home loan borrowers higher fees.[25]

A Denver attorney, Qusair Mohamedbhai, filed a federal lawsuit in March 2005. A member of both the Colorado and Wyoming state bars, and in good standing with excellent credit, he alleged that he was denied a checking account by Commercial Federal Bank in May 2004 and that the bank racially profiled and slandered him. Mohamedbhai was apparently under the initial impression his denial was routine, until he learned that Genevieve Babcock-Elder of Colorado Cheque Connection had actually spelled out his name to a seminar audience on banking and terrorism during which she publicly claimed credit for "thwarting a terrorist from getting a checking account." Mohamedbhai, who was born in Edmonton, Alberta and "looks Middle Eastern," but is of Indian descent and is a permanent legal resident of the United States, was characterized by Babcock-Elder as having "moved around a lot," "funneled $160,000 for terrorism eight years earlier through the Colorado National Bank and had returned to the scene of the crime." Babcock-Elder also loosely associated Mohamedbhai to the terrorists who expedited 9/11 by suggesting that because his Social Security card was originally issued in Florida, where the terrorists took flying lessons, he was connected to the group.[26] In fact, Mohamedbhai had no involvement in any of the suggested activities.

While large banks like Fleet have to balance the requirement to file SARs and CTRs based on suspected suspicious activity, their responsibility to protect the privacy and rights of their account holders still remains. When a customer's name is NOT on a federal list, the bank ultimately has the discretion whether to file a SAR or CTR. Often, it is because of this discretion that discrimination occurs.

FBI Special Agent Colleen Rowley observed in her questioning in terrorism investigations, "[t]he vast majority of the one thousand plus persons 'detained' in the wake of 9/11 did not turn out to be terrorists ... [she admits] the balance between individuals civil liberties and the need for effective investigation is hard to maintain even during so-called normal times, let alone times of increased terrorist threat or war. It is, admittedly, a difficult balancing act. But from what I have observed, particular vigilance may be required to head off undue pressure to detain or 'round up' suspects, particularly those of Arabic origin."[27]

---

25. *Id.*

26. *Man Denied Account Sues Bank, Alleges Racism*, www.thedenverchannel.com/print/4313737/detail.html.

27. AMERICAN CIVIL LIBERTIES UNION, HOW "PATRIOT ACT 2" WOULD FURTHER ERODE THE BASIC CHECKS ON GOVERNMENT POWER THAT KEEP AMERICA SAFE AND FREE (2003), *available at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12161&c=206 (citing to *Full Text of FBI Agent's Letter to Director Mueller*, N.Y. TIMES, Mar. 5, 2003).

In the three years since Patriot Act I was passed, racial profiling based on assumptions about national origin have re-emerged as acceptable law enforcement and societal behavior. Particularly those of Arab and Muslim descent, or those who *appear* to be of Middle Eastern origin, have noted increased incidents of disparate treatment as a result of the terrorist attacks of 9/11.[28] While profiling may seem reasonable in today's anti-terrorism environment, this practice is not acceptable under the constitutional protections of a free nation. While building the ideology of the USA Patriot Act, our legislators ignored the racial and privacy implications of Patriot Act I. They are considering compounding that mistake in Patriot Act II. Perhaps the most overwhelming constitutional dangers were created by the regulatory responses of banks to Patriot Act I.

Policies adopted by banks in response to the demands of the Bank Secrecy Act, the Annunzio-Wylie Anti-Money Laundering Act,[29] Patriot Act I and the Proposed Domestic Security Enhancement Act referred to as Patriot Act II[30] promote institutional racism. Now, not only must people of color still submit to unequal and unconstitutional treatment by law enforcement on the street, but denial of privacy at the teller window is further eroding their constitutional rights. Because of this potential harm, banks, at a minimum, should be required to find some level of probable cause before filing a SAR or CTR, or subjecting an account holder and their banking activities to government intrusion. The Right to Financial Privacy Act (herein RFPA)[31] generally prohibits disclosure of a customer's banking records to the government without the customer's consent. However, the Bank Secrecy Act has a markedly different threshold, and states that there is no right to privacy in an individual's bank records. The U.S. Supreme Court has held that there is no legitimate expectation of privacy in bank records.[32] Under Patriot Act I, banks are forbidden from disclosing their CTR and SAR reporting activities to their account holders. It is the numerous exceptions created by this maze of legislation that allows unprecedented exposure of individual financial privacy.

How should we balance the government's need to maintain a safe country with our citizens' rights to privacy? Should we engage in a cost

---

28. *See* AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION TO PROVIDE LEGAL HELP TO MUSLIMS AND ARABS CAUGHT UP IN NEW ROUND OF FBI QUESTIONING (2004), http://www.aclu.org/safefree/general/18508prs20040805.html. (announced in response to a recent announcement by Attorney General John Ashcroft and FBI Director Robert Mueller that the FBI would launch a new round of dragnet-like interviews in Arab and Muslim communities nationwide).

29. Annunzio-Wylie Anti-Money Laundering Act, 102 Pub. L. No 550, § 106 Stat. 4044 (1992) (codified in several sections of 12,18, 31, and 42 U.S.C.).

30. *See Interested Persons Memo: Section-by-Section Analysis of Justice Department draft "Domestic Security Enhancement Act of 2003,"* also known as PATRIOT Act II (2003), *available at* http://www.aclu.org/safefree/general/17203leg20030214.html.

31. The Right to Financial Privacy Act, 12 U.S.C. §§ 3401–342.

32. *See* United States v. Miller, 425 U.S. 435, 443 (1976).

effective analysis to determine if profiling is justified? How should one measure the injury to someone who is mistaken for a terrorist resulting in their bank account being frozen , or has a SAR or CTR mistakenly filed? It is logical that if law enforcement is looking for Middle Eastern terrorists they will certainly heighten their scrutiny of people from the Arab world. However, the racial profiling of Blacks has not served to curtail drug trafficking in this country.[33] In practice, how does a teller,[34] an operations manager or a bank branch manager draw a conclusion as to whether to approve a $10,000 transaction for an individual and/or file a corresponding SAR or CTR? By a glance, a twenty second conversation, or an evaluation of an individual's clothes, demeanor, race or ethnicity, or a cursory review of the transaction itself? This process of practical application of the BSA is what can create misjudgments.

Bank reporting policies are dangerous not because the policies are wrong, but because these policies do not, or perhaps cannot, factor in the decision making ability and biases. New tellers and seasoned tellers alike are trained in these policies, but both still have little experience applying them.

The "little people" like bank tellers and TSA (Transportation Security Administration) screeners are on the front lines of terrorist inspection in this country. Consider the operations manager who harbors secret biases against those of Middle Eastern descent. What about the teller who simply does not understand the threshold of cash or criteria for reporting a "suspicious act?" Or perhaps these incidents happen maliciously, because

---

33. *See* Human Rights Watch, *Punishment and Prejudice: Racial Disparities in the War on Drugs* (2000) and Human Rights Watch, *Justice on Trial: Racial Disparities in the American Criminal Justice System* (2002) (on file with author); Ronald H. Welch & Carlos T. Angulo, Leadership Conference on Civil Rights, Leadership Conference Education Fund, April 2000 7(on file with author)(explaining that most drug users are not Black, but Blacks represent 13% of drug users nationwide, in proportion to their share of the population, and that escalating pressure from the war on drugs has led some police officers to target people of color whom police believe to be disproportionately involved in drug use and trafficking). John Lamberth, *Report of John Lamberth, Ph.D., available at* http://www.stat.uiowa.edu/~gwoodwor/statsoc/lectures/w2/lamberth.html (finding that on I-95 in Maryland, 28.4% of Black drivers and passengers who were searched were found with contraband and 28.8% of White drivers and passengers who were searched were found with contraband—thus the probability of finding contraband was the same for Blacks and Whites); STATE OF NEW JERSEY, SELECTED HIGHLIGHTS OF THE INTERIM REPORT OF THE STATE POLICE REVIEW TEAM REGARDING ALLEGATIONS OF RACIAL PROFILING (1999), *available at* http://www.aele.org/NJprofil.html (stating that the "hit rates" at which contraband was found among those searched did not differ significantly by race . . . to date the evidence indicates that Blacks and Latinos are no more likely than Whites to be in possession of narcotics or other contraband); RAMIREZ, *supra* note 2, at 10 (indicating that Blacks and Latinos are no more likely than Whites to be in possession of narcotics or other contraband).

34. The U.S. Department of the Treasury, Office of Foreign Assets Control considers tellers to be a bank's "first line of defense against violative personal remittances." 1378 PLI/Corp 627, 652 (July 2003).

the bank teller or TSA screener's duties are their first or only exposure to power over others. Regardless, because of civil and criminal penalties which can be levied if mistakes are made, these individuals are going to err on the side of caution. A bank can be fined up to $1 million if they do not act decisively to stop an illegal flow of money or freeze an account. That translates into real pressure for an employee at the teller window or on the floor of the bank branch office.

Those who work in the front lines of carrying out bank policy are members of a society in which insidious racism thrives. They are, like all of us, operating with the same standards of behavior that exist in the larger society. For years, local and national leaders claimed there was no evidence of selective enforcement of the law, no evidence that Blacks were being profiled and stopped in their automobiles for imaginary violations of the law. Even when irrefutable proof was presented to the contrary, there was no response. America did not care for a very long time. To the great surprise of some, in 1989 the incidents of racial profiling on New Jersey highways became national news. In some circles the existing evidence was debated, but disregarded, partially because it was people of color who were affected.

Should we care now? As vehemently as we may deny the continued existence of institutional racism, there is substantial evidence it remains. Profiling exemplifies the Constitutional dangers when laws are applied unequally to different ethnic groups. Legitimizing racial profiling in a world where we all, including bank officers and employees, use discretion tainted by personal prejudices, gives the government the power to label people of color as "suspicious." Patriot Act I is the first born child of The Foreign Intelligence Surveillance Act.[35] FISA arose from J. Edgar Hoover's obsession with Martin Luther King, Jr. and other civil rights leaders. Patriot Act I allows every law enforcement official—from the CIA to the local sheriff—the right to rely on these broader domestic surveillance rules[36] to root out terrorists, resulting in the harassment of, and harm to, people of color. Giving local drug enforcement policemen broader powers is in part what led to the killing of Amadou Diallo.[37] Local police flexing their discretionary powers is what led to the unabashed arrogance it took for the attempted murder by sodomy of Abner Louima.[38] When the Judiciary, our legislators, and the people of this country accepted racial profiling as a lawful tool to fight the drug war, they acquiesced in its lawfulness to fight terrorism.

However, could class be more of the issue? Until very recently private banking was a loophole in the broad swath of protection BSA

35. 50 U.S.C. § 1861 (1978).

36. USA Patriot Act § 215, 50 U.S.C. § 1861(2001)

37. *See In re* Grand Jury Investigation of Death of Diallo, 688 N.Y.S.2d. 386 (N.Y. Sup. Ct. 1999).

38. Louima v. City of New York, 2004 WL 2212093 (E.D.N.Y. 2004).

intended to create. Publicly, the wealthy are not thought of as having any connection to terrorism, but the facts suggest otherwise. Government intelligence agencies allege wealthy U.S. citizens *have* been used by terrorists to launder money. The Sami Amin Al-Arian scheme aside,[39] wealthy bank customers whose accounts regularly reflect large cash deposits and withdrawals of the threshold CTR and SAR reporting amounts, carry out their business freely without breach of their privacy or judgments regarding the objective of their bank transactions. Even with new scrutiny, private banking transactions rarely produce the filing of a SAR or CTR, irrespective of the account holders ethnic origin. Most often, "Know-Your-Customer"[40] policies provide methods to obviate the banks of having to file SARs or CTRs for these customers,[41] and therefore, powerful or wealthy bank consumers are not often faced with this particular possible loss of their constitutional privacy rights.[42]

Unfortunately, in the process, basic Constitutional costs are being paid by all Americans as a result of the practical problems created when banks use racial profiling in a hapless attempt to thwart terrorism.

II. COMPROMISING THE REPORTING DEVICES

A. *Generating Cash Transaction Reports—CTRs*

Patriot Act I requires the filing of a CTR to FinCen[43] by financial institutions and by any person engaged in a (non-financial) trade or business if they receive more than $10,000 in any currency in one transaction or multiple related transactions totaling more than $10,000 during one business day. The CTR is required by law to contain the name of the depositor, beneficial owner of the account if different than the depositor, and address and telephone number of the depositor. CTRs were a tool initiated in 1970 by the Bank Secrecy Act, but now closely associated with both anti-money laundering as well as terrorism. The Department of

39. *See* Edmund L. Andrews, *U.S. and Saudis Act to Freeze Charity's Assets*, N.Y. TIMES, Jan. 23, 2004, at A4; Glenn R. Simpson, *U.S. Links Scholar to Possible Terror Funding*, WALL ST. J., Mar. 17, 2003, A4; United States v. Al-Arian, 267 F. Supp. 2d 1258 (M.D. Fla. 2003).

40. Pursuant to BSA and § 326 of the Patriot Act, the Secretary of the Treasury issues specific minimum "Know Your Customer" standards, requiring banks to attempt to make reasonable and practical efforts at verification of new customers; maintain records of the information used to verify identification; and consult lists of known terrorists. Online brokers who do not meet or speak with their clients are required to use a computer system which flags suspicious activity and to acquire customer information by other means, such as through electronic databases like the credit reporting agencies.

41. *See* DEP'T OF TREASURY FORM TD F 90-22.53, *available at* www.fincen.gov.

42. *But see* U.S.A. Patriot Act, §§ 312(a)(3)(B), 363 (2003).

43. FINANCIAL CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, I.R.S. FORM 8300 (2004), http://www.fincen.gov/forms/fin8300_cashover10k.pdf.

Treasury, Office of Foreign Assets Control (OFAC) tends to use CTRs differently than SARs are used pursuant to the Bank Secrecy Act.

> "OFAC programs have historically emphasized 'freezing' rather than 'seizing' assets to achieve foreign policy goals. Blocking provisions are often 'protective,' [or political] as when Kuwaiti assets were preserved from Iraqi aggression or Norwegian and Danish assets were shielded from the Nazi invasion of those countries. Freezing is also used to create and preserve a "pool" of assets to satisfy the interests of injured claimants and creditors against parties under sanctions."[44]

The filing requirements for CTRs are fairly consistent and straightforward, but the boundaries of what constitutes "suspicious" activity and therefore requires the filing of a SAR continue to be highly subjective and capricious.

A CTR for each transaction (deposit, withdrawal, exchange of currency, or any other payment or transfer made to or through any financial institution) involving more than $10,000 in currency must be filed by the financial institution with the Treasury Department Financial Crimes Enforcement Network (FinCEN) and are also often filed with the Internal Revenue Service. The CTR must contain the name of the depositor, beneficial owner of the account if different than the depositor, and address and telephone number of the depositor.

Patriot Act I also greatly expanded the definition of "financial institutions" to include credit unions, casinos, money service businesses, money transmitting businesses, securities brokers-dealers, futures commission merchants, commodity trading advisors, commodity brokers, and commodity pool operators registered under the Commodity Exchange Act.[45] All of these financial institutions must now file CTRs. Certain other businesses are considered financial institutions under 31 U.S.C. 5312: pawnbrokers, travel agencies, insurance companies, dealers in precious metals, stones or jewels, telegraph companies, loan and finance companies, persons involved in real estate closings and settlements, auto, airplane and boat dealers. Partly as a result of expanding the definition of a "financial institution," and for a multitude of other reasons, approximately thirteen million CTRs are filed each year, while bankers complain that they are "virtually useless."[46] Financial institutions have specific guidelines via the Treasury Department as to when they are required to file CTRs. These banks may, however, exempt certain customers from CTR reporting requirements.

---

44. 1378 PLI/Corp 627,653 (July 2003).

45. Commodity Exchange Act, 7 U.S.C. § 1, et seq.

46. Krysten Crawford, *Drawing a Bead on Terrorism Funds: Financial Fight May Be Mission Impossible*, LEGAL TIMES, Jan 28, 2002, at 1.

Title III of Patriot Act I is titled "The International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001"[47] and provides the authority for the filing of both CTRs and SARs.[48] Funds which are the subject of a CTR are forfeited as part of any sentence for criminal or civil[49] violations of currency reporting rules.

B. *Creating Suspicious Activity Reports—SARs*

If in an individual transaction a bank receives $5,000 in currency, a SAR is required to be filed. The reporting threshold for transactions conducted at points of sale for money services businesses[50] is $2,000.[51] The SAR is forwarded to the U.S. Department of the Treasury, the IRS, FinCEN, and any other governmental agency that requests the SAR based on a need related to a terrorist investigative issue.[52] Terrorist Financing was added as a suspicious activity characterization in July 2003; between July and December [2003], 495 SARs were filed with this characterization box marked.[53]

"A SAR must be filed with the Department of the Treasury under the following circumstances:

> Insider abuse involving any dollar amount that the financial institution detects or any known or suspected federal criminal violation, committed or attempted against the institution when the suspect is a director, officer, employee, agent, or other institution-affiliated party.
>
> Violations aggregating $5,000 or more in funds or other assets where a suspect can be identified.

---

47. U.S.A. Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C., 22 U.S.C., 31 U.S.C., 47 U.S.C., and 50 U.S.C.).

48. These reports are submitted through a secure network managed by the financial crimes communication center and the government-wide data access service, who catalog information for purposes of rapid retrieval and prompt initial review of all suspicious activity reports.

49. 18 U.S.C. §§ 981–82 (2006).

50. 31 C.F.R. § 103–15 (2006)

51. 31 C.F.R. § 103–20 (2006).

52. FinCEN has implemented an optional system to promote the sharing of information among financial institutions. Patriot Act Communications (PACS) allows banks to expeditiously file BSA reports over the internet using a secure connection. It is hoped that PACS will streamline the process, reduce the reporting costs for banks and other financial institutions, and make the information available to the intelligence and law enforcement agencies faster.

53. *See* http://www.fincen.gov.

> Violations aggregating $25,000 or more in funds or other assets even though there is no substantial basis for identifying a possible suspect or group of suspects.[54]
>
> There are currently twenty-two categories under which SARs can be filed."[55]

In general, a SAR should indicate five basic elements of information: "Who is conducting the suspicious activity? What instruments or mechanisms were used to facilitate the suspicious transaction(s)? When did the suspicious activity take place? Where did the suspicious activity take place? Why does the SAR filer think the activity is suspicious?"[56]

As with CTRs, Title III of Patriot Act I significantly increases the number and types of financial institutions that are required to file SARs. Securities broker-dealers, money transmitting businesses, and commodities brokers registered with the SEC must now submit SARs. So, too, must futures commission merchants, commodity trading advisors, and commodity pool operators registered under the Commodity Exchange Act.[57]

FinCEN publishes a national bulletin advising financial institutions on trends and patterns in money laundering, and supplies examples of suspicious transactions that could "highlight activities or issues that appear significant based on such factors as number of reports, number of financial institutions filing similar reports, aggregate dollar values, geographic distribution, and especially recurrent patterns of activity identified in SAR narratives."[58] SAR Information Bulletins are designed to alert financial institutions of the type of criminal activities that have been and should be reported using SARs. The actual SAR form provides an opportunity to report twenty different types of suspicious activities.[59] While reporting the vast majority of these "suspicious transactions" is of significant value, some generalizations drawn from common reported transactions present poten-

---

54. Transactions aggregating $5,000 or more that involve potential money laundering or violations of the BSA, or where the transaction has no business or apparent lawful purpose or is not the sort of transaction in which the particular customer would normally be expected to engage, and the bank knows of no reasonable explanation for the transaction after examining the available facts.

55. *Id.* at 2.

56. *Id.*

57. Commodity Exchange Act, 7 U.S.C. § 1, et seq. (2006).

58. Financial Crimes Enforcement Network, Dep't of the Treasury, *SAR Bulletin: Information Drawn From the Suspicious Activity System* 5 (2002), *available at* http://www.fincen.gov/sarbul0201-f.pdf [hereinafter *SAR Bulletin*].

59. A financial institution can check boxes which indicate structuring/money laundering, bribery/gratuity, check fraud, check kiting, commercial loan fraud, computer intrusion, consumer loan fraud, counterfeit check, counterfeit credit/debit card, counterfeit instrument, credit card fraud, debit card fraud, defalcation/embezzlement, false statement, misuse of position or self dealing, mortgage loan fraud, mysterious disappearance, wire transfer fraud, terrorist financing, and identity theft.

tial dangers. Take, for example, Case 5 presented as a classic situation meriting scrutiny. The example describes a "pattern of cash deposits below the CTR reporting threshold generated a SAR filing by a U.S. depository institution. Deposits were made to a foreign currency exchange on a daily basis totaling $341,421 over approximately a two and one-half month period. During the same period, the business initiated ten wire transfers totaling $2.7 million that were sent to a bank in the United Arab Emirates. When questioned, the business owner reportedly indicated he was in the business of buying and selling foreign currencies in Iran, the Persian Gulf states, and other countries in the Middle East, and his business never generated in excess of $10,000 a day. CTRs for a three year period reflected cash deposits totaling $137,470 and withdrawals totaling $29,387. The business owner and the cash out transactions were conducted of nationals of countries associated with terrorist activity. Another U.S. institution filed a SAR on this individual indicating an $80,000 cash deposit, which was deemed usual for his profession. He also cashed two negotiable instruments at the same depository institution for $68,000 and $16,387 according to CTR filings."[60] These transactions are indeed an issue. But it is mainly the high deposits over the two month period and the wires between the U.S. and the United Arab Emirates of $2.7 million that should raise ire. The "pattern of cash deposits below the CTR reporting threshold" and cashing a $68,000 and $16,387 instrument could apply to anyone conducting a personal or business transaction.

The indicators leading to the filing of a SAR cited in this bulletin are entirely relevant and directive:

- Use of a business account that would normally not generate the volume of wire transfer activity, into and out of the account, as reported;
- Apparent structured, daily deposits to business account;
- Wire transfer activity within a short period following deposits;
- Beneficiary account in a "problematic" country;
- Currency exchange buying and selling foreign currencies from various countries in the Middle East;[61]

However, several additional indicators cited may suggest racial profiling or create, at a minimum, a propensity to over-report.[62] At the very

60. *SAR Bulletin*, *supra* note 58, at 4.

61. *Id.* at 4–5.

62. Financial Crimes Enforcement Network, Dep't of the Treasury, *Industry Partnership Results in Valuable Investigative Leads*, FINCENNEWS, Dec. 17, 2003, *available at* http://www.fincen.gov/314arelease_121703.pdf (claiming to have processed 188 requests submitted by ten federal agencies in response to financial institution searches on recent account and transaction records about individuals, entities, and organizations engaged in,

least, these indicators suggest that more definitive guidelines for a SAR filing need to be established. Following are the additional pertinent directives cited as "indicators leading to the filing of a SAR:"

- Transactions at a level not commensurate with stated occupations.
- Business account activity conducted by nationals of countries associated with terrorist activity with no obvious connection to the business;
- Apparent structured, daily deposits to business account;
- Wire transfer activity within a short period following deposits;
- Apparent intent to circumvent wire remittance company's internal requirements for presentation of identification through purchase of money orders in small amounts;
- Movement of funds through a Financial Action Task Force (FATF) designated non-cooperative country or territory such as the Cook Islands, Dominica, Egypt, Grenada, Guatemala, Hungary, Indonesia, Israel, Lebanon, Marshall Islands, Myanmar, Nauru, Niue, Philippines, Russia, St. Kitts and Nevis, St. Vincent and the Grenadines, and Ukraine.
- Use of sequentially numbered money orders;
- Funds generated by a business owned by nationals of countries associated with terrorists activity
- Use of a business account to make payments to a brokerage firm;
- Same day transactions at the same depository institution using different tellers;[63] and so forth.

These kinds of disputable guidelines further complicate the discretionary decisions of front line bank employees because they are so open to interpretation.

Bankers dislike SAR filings because the government's indicators are inconsistently applied from bank to bank, and from market to market, making it difficult for bank personnel to determine when a SAR needs to be filed. After legions of hearings, directives, discussions and interpretations of BSA and Patriot Act I regulations, banks are still unsure and

---

or reasonably suspected of engaging in terrorist acts or money laundering activities and to have discovered numerous suspect accounts despite no clearly documented arrests stemming from a particular SAR or CTR during that time period).

63. *SAR Bulletin*, *supra* note 58, at 2–5.

anxious about the compliance advice they receive. In addition, banks complain that different branches of the government are reviewing SARs for different reasons, thereby making inconsistent demands about what data should be supplied. SARs are often inaccurate and incomplete, making them inappropriate for FinCEN to act upon.[64] Even the Office of the Comptroller's 1700 examiners, with currently about 1800 OCC examiners, are inconsistent in their evaluation of Bank compliance.[65] In addition, banks have become wary of complying with the government's regulations due to the lack of confidentiality surrounding the filing of SARs. Leaks of SARs from several banks have been documented,[66] increasing the

---

64. *See* James F. Sloan, U.S. Dep't of Treasury, *FinCEN: Reliability of Suspicious Activity Reports* (Dec 18, 2002), www.ustreas.gov/inspector-general/audit reports/2003/oig3035.pdf (reporting that many of the 505,000 SARs completed by financial institution personnel and filed between April 1996 and December 2000 were either duplicated or were inaccurate or incomplete. Information omitted from the forms included names of the suspects, identification of what the suspected defense was, and the filing institution's regulators); U.S. Dep't of the Treasury, Fin. Crimes Enforcement Network, *FinCEN Awards BSA Direct Contract to EDS,* FINCENNEWS, (June 30, 2004), http://www.fincen.gov/bsadirectcontractaward.pdf (announcing a database of national bank-filed SARs with enhanced search and reporting capabilities called BSA Direct, to be "fully operational by October 2005," that the contract to design, develop, implement, web host and provide support services was awarded to EDS, and that "BSA Direct is designed to support FinCEN's administration of and compliance with the Bank Secrecy Act."); *Risk Management and Regulatory Failures at Riggs Bank and UBS: Lessons Learned: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Financial Services, 108th Cong. 17 (2004)* (statement of Daniel P. Stipano, Deputy Chief Counsel, Office of the Comptroller of the Currency).

65. *Banks, Regulators Grapple With SAR Filings,* AM. BANKER THE FIN. DAILY, June 8, 2004, at 12. (reporting that examiners are telling bankers that the number of reports they file—not the quality or usefulness of those reports—is a key factor in assessing compliance). There are approximately 300 examiners onsite at the largest national banks engaged in continuous supervision of all aspects of their operations; 40 full time employees were dedicated in 2003 to BSA supervision; three full time BSA compliance specialists are in the Washington D.C. headquarters office of the OCC dedicated to developing policy, training, and assisting on complex examinations; and there is a full time fraud expert responsible for tracking the activities of offshore shell banks and other vehicles used to defraud banks and the public; supplemented by dozens of attorneys in OCC district offices and the Washington D.C. headquarters who work on compliance matters. In 2003, the OCC conducted approximately 1,340 BSA examinations of 1,100 institutions and since 1998, 5,700 BSA examinations of 5,300 institutions have been completed. *See* Statement of Daniel P. Stipano, *supra* note 64, at 6–7 (testifying to the amount of manpower engaged in supervision of aspects of the operations of the largest national banks, BSA supervision and compliance, and development of policy and to the approximately 1,340 BSA examinations of 1,100 institutions and since 1998, 5,700 BSA examinations of 5,300 institutions have been completed by the OCC).

66. *Banks, Regulators Grapple With SAR Filings, supra* note 65, at 12 (quoting speculation that the Washington bank may be acquired):

> The issue first surfaced in an article in the April 7 issue of Newsweek which used information from, and quoted, SARs filed by Fleet National Bank of Boston. An article in Sunday's issue of The Washington Post used information

likelihood of banks who rightfully do not disclose their SAR policies receiving negative press, and help criminals to learn to mask their banking activities in ways which avoid SAR filings. Furthermore, these leaks have promoted the public perception that there is illegal activity associated with account holders , thereby increasing the fears of bankers, and possibly chilling future filings.

Almost uniformly, bankers note that if they were privy to the criminal investigations of these various government agencies, they would be better able to identify the activity and information that interests law enforcement. If banks are unaware of the complexities of terrorist finance schemes, then their analysis cannot be adequate. Without *real guidelines* from the government, the alternatives that bankers will resort to when deciding how to identify terrorists will likely encourage dangerous tactics like racial profiling.

Beginning in 1987, the BSA required banks to implement and maintain anti-money laundering devices.[67] Under Patriot Act I, anti-money laundering programs commensurate with the size, location and activities of a financial institution must be formally maintained. One administrative difficulty at the time Patriot Act I was enacted was that its requirements were extended to a wider range of financial institutions, such as broker-dealers, casinos, investment companies and organizations such as check cashing outlets, money service businesses, and Western Union.[68] Thus, CTRs and SARs used to originally thwart money laundering would not only be used to implement terrorists devices, but would also have a much larger impact on the country's overall financial transactions.

In addition, if the Secretary of Treasury determines that a financial institution, an account, or a particular transaction is of "primary money laundering concern," the Secretary could require the bank to "maintain additional records or make additional reports in connection with those transactions; identify the foreign beneficial owners of certain accounts; identify the customers of foreign banks who use interbank correspondent accounts and payable-through accounts; and restrict or prohibit the opening or maintaining of these payable-through or correspondent accounts."[69] While this may all have been well-intentioned by the drafters of Patriot Act I, they failed to consider how the problem of over-reporting from all

---

and quotes from more than a dozen SARs filed by Riggs Bank. Neither article revealed the source of the reports.

See also Some Fear SAR Leaks Will Lead to Fewer Filings; AM. BANKER THE FIN. DAILY, Apr. 23, 2004 at 3 (" 'Once financial institutions suspect that highly sensitive information they are filing on a SAR might be publicly disclosed, they may be reticent to be as candid and forthcoming as they have been in the past.' said Peter Dijinis, a former top official at FinCEN.").

67. 31 U.S.C. § 5318(h) (2006).

68. USA Patriot Act § 352 (a)-(c) (2001).

69. *Id.* at § 311 (codified as amended in 31 U.S.C. § 5318A(c)(1), § 5318A(b)(2003)).

the newly required financial institutions on matters of both money-laundering and terrorism would bog down the current reporting system.

Extending the requirements of the BSA to a larger number of financial institutions, as well as adapting this legislation to report terrorism, fails to take into consideration that a significant portion of the sources of terrorists funding has yet to be identified, let alone tracked to the sources from which it originated. These funds have been determined to come from such a vast array of diversified and legally operated businesses (from travel agencies, internet companies, charitable corporations, to small mom-and-pop grocers and car dealers), in locations both foreign and domestic, that they are next to impossible to track.

Simply, the system that regulates SARs is just too riddled with problems. Most SARs filed are incomplete, the sheer number of SARs filed is overwhelming, and the directives of when to file a SAR are too broad. This overburdens the Treasury Department which ultimately complicates the government's ability to successfully utilize CTR and SAR obtained information. FinCEN claims the solution is its Artificial Intelligence or AI[70] system. Few in the banking industry believe that.

III. CONSTITUTIONAL CONSEQUENCES OF THE BANK SECRECY ACT

Those who place civil liberties as more important than the benefits that might result from government intrusion oppose an increase in the centralization of Americans' financial information, as long as it exists without drastic protections against the possible government misuse of that knowledge. Squarely in the path of that argument is the U.S. Supreme Court's position that there is no Fourth Amendment expectation of privacy in a person's bank records when a governmental agency has an interest in examining those records.[71]

---

70. AI is a complex computer system that provides the ability to process vast amounts of data, enabling our analysts to explore the sets of links it has established. The customized programs and algorithms developed by FinCEN's computer scientists allow the AI's KDD, or Knowledge Discovery Databases, to pull in relevant information from the universe of CTR data. The system then connects disparate pieces of information, such as banking transactions and accounts, and this linking process reveals patterns of financial transactions that we know are used to launder money or to perpetrate other crimes. Thus we can find potential suspects during the AI analysis who might have gone undetected. The AI system has linked together common elements from 90 different currency transaction reports. The system has honed in on these particular CTRs because the activity reveals a suspicious pattern of cash deposits which simply do not fit the normal profile of a small grocery store. *Treasury, Postal Serv., and Gen. Gov't Appropriations: Hearing Before the Subcomm. on Treasury, Postal Serv., and Gen. Gov't of the H. Comm. on Appropriations*, 105th Cong. 113-4 (1997)(statement of Stanley E. Morris, Director, FinCen).

71. *See Miller*, 425 U.S. at 443.

The BSA has become the cornerstone of the federal government's terrorist and anti-money laundering controls.[72] The Act requires banks and financial institutions to monitor and report certain financial transactions to the Secretary of the Treasury.[73] It primarily affects the conduct of banks in the retention of records,[74] recordkeeping and procedures.[75] Generally, the purpose of the BSA is to ensure that banks—and other financial institutions regulated by the Office of the Comptroller of Currency,—provide all relevant information to law enforcement concerning anti-money laundering and terrorist financing in the form of CTRs and SARs expeditiously.

The implementation of the BSA "does not constitute an illegal search and seizure in violation of the Fourth Amendment,"[76] neither does the BSA deprive financial institutions of due process by its recordkeeping and reporting requirements.[77] Yet, the Department of Treasury has used Patriot Act I and the BSA to pass a plethora of regulations designed to intercept the financing of terrorist activity and the identification of terrorists.

Since its initial passage in 1970 and the required implementation of BSA compliance procedures in 1987, bankers have made it clear they do not like the BSA. Community banks[78] especially are overwhelmingly burdened by the demands of BSA reporting. FDIC Vice Chairman John Reich admits, "The volume and complexity of existing banking regulations, coupled with new laws and regulations, may ultimately threaten the survival of our community banks . . ."[79] Even members of the House Financial Services Committee continue to question whether BSA reporting requirements are too rigid, and whether the Treasury Department is really utilizing the data that is being provided. Regulators again made adjustments in the reporting requirements at the end of 2004.[80] Rep. Scott

---

72. *See* 12 U.S.C. §§ 1829(b), 1951–1959 (2003); 31 U.S.C §§ 5311–5322 (2003).

73. *See* 31 U.S.C. § 5312(a)(2) (2003) (defining a "financial institution" as including banks, depository institutions, casinos, card clubs, money services businesses, broker-dealers and investment companies).

74. *See* 12 U.S.C. § 1829(b) (2003).

75. *See id.* at § 1953.

76. *See* Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 45–54 (1974).

77. *See* § 31 C.F.R. 103.22(b)(1).

78. Community banks are regional financial institutions, typically with assets of approximately $5 billion or less, which serve and market to a specifically designated segment of the communities in which they do business, most notably offering highly community-oriented banking, serving local and regional businesses and the social and financial needs of their customers.

79. Michelle Heller, *Clash on Bank Secrecy Act Compliance*, AM. BANKER THE FIN. SERV. DAILY, May 13, 2004.

80. BSA REPORTING REQUIREMENTS, U.S. TREASURY DEPARTMENT (2004), *available at http://www.occ.treas.gov/ftp/bulletin/2004-50.txt*; OCC 2004-50, OCC BULLETIN BANK SECRECY ACT/ANTI-MONEY LAUNDERING ACT OF 1970, *available at* OCC 2004-50; ANN F.

Garrett asked officials from the Treasury Department and the Federal Deposit Insurance Corp., "Is there any consideration to raising the $10,000" trigger for banks to file a currency transaction report "to a more realistic, higher number like $20,000 or $30,000?"[81]

BSA requires banks to peer into the financial lives of its customers. Through personal bank records, personal lives are opened to inspection; personal political party affiliation, religious affiliations, eating and leisure habits, cash spending tendencies, personal shopping habits, travel preferences, music and video delights, perhaps even dating lives or marital difficulties. We live in a world where, increasingly, personal lives can be tracked through the financial transactions . But in many ways, we have been able to limit who accesses this information.[82] These limits have been impeded under Patriot Act I.

Problems and complaints connected to the filing of SARs continue to mount. Yet, suspicious activity remains extremely difficult to define. A simple act of depositing checks in separate envelopes in one transaction, or making a one-time withdrawal over $5,000, or the deposit of a payroll check from a company which surfaces on a watch list may trigger a SAR. When an account is flagged for suspicious activity, the account holder is not told why, thus leaving no opportunity to offer a justification for the habit or occurrence which ignited the concern and retrieve one's reputation; a reputation which becomes increasingly valuable as the account holder attempts to relocate her account to another financial institution.

Millions of hours of manpower at banks are being diverted at all levels, from tellers who file the SARs or CTRs, to senior managers who also have compliance responsibilities. Ideas to expand bank business, meet customer needs, promote products, and manage personnel all take a back seat to regulatory compliance in some banks. Not only are labor resources being lost, but billions of dollars must now be spent on BSA compliance training, software, hardware, telephone connections to meet the requirements of the SARS[83] reporting system, and outside compliance support

---

JAEDICKE, COMPTROLLER OF THE CURRENCY, OCC BULLETIN: BANK SECRECY ACT/ANTI-MONEY LAUNDERING (2004), http://www.occ.treas.gov/ftp/bulletin/2004-50.doc

81. *See* Heller, *supra* note 79.

82. *See* Stark v. Connally, 347 F. Supp. 1242, 1248, (N.D. Cal. 1972) stating that:

> banks have traditionally returned, either directly or through the clearing house, all checks each month to the original drawer of the checks. It would seem reasonable therefore, for the drawer of the check to regard himself as the real owner of his checks, subject only to normal banking processing, and to expect that detailed information shown only on the face of his checks will not be automatically broadcast throughout the vast government bureaucracy without at least some notice, summons, subpoena or warrant in connection with some legitimate pending inquiry.

83. *The Financial Services Regulatory Relief Act of 2005: Hearing on H.R. 3505 Before the Subcomm. on Financial Institutions and Consumer Credit of the H. Comm. on Financial*

such as accountants, attorneys and consultants. On November 10, 2004, federal regulators published a Bank Secrecy Act (BSA) examination guide which attempts to reconcile the conflicts between the BSA and Patriot Act I inherent in SARs. In an OCC Bulletin of that date citing 12 C.F.R. 21.11 formally recognized "that the decision to file a SAR is an inherently subjective judgment."[84] The Bulletin gave the following guidance: "If the bank has no *reasonable explanation* for an unusual transaction after evaluating the facts, it should be considered suspicious, and the bank should file an SAR."[85] This may suggest that banks have a duty to explore the possibility of a "reasonable explanation" for a transaction *before* filing a SAR. If this is a sound interpretation of OCC 2004–50, it would go a long way toward alleviating random discretion of bank employees, and lessen the likelihood that Muslim and Middle Eastern account holders would be racially profiled.

In 2004, the Office of Terrorism and Financial Intelligence (TFI) was created at the Department of the Treasury. TFI is charged with the responsibility of the financial war on terror, the integrity of the American financial system, fighting financial crime, enforcing economic sanctions against rogue nations and assisting in the hunt for Iraqi assets.[86] The Executive Office of Terrorist Financing and Financial Crimes, FinCEN, and the Office of Foreign Assets Control, along with certain reallocated resources from the Treasury Department were all brought under TFI. Bankers were opposed to the creation of TFI because they see it as only adding to the confusion.

As recently as June 2004, FinCEN's Director, William J. Fox, hailed the importance of FinCEN and the BSA as the "financial front of the war against terrorism." He expressed his belief that "money does not lie. A good part of the time, financial intelligence is actionable intelligence. It can be extremely useful for identifying, locating and capturing terrorists and defining their networks . . . and stops the flow of money to terrorists . . . which in turn serves to halt or impede terrorists operations."[87] Unfortunately, this is not what has happened. The Bush Administration would like us to believe Patriot Act I has made a real difference in our efforts to seize terrorist dollars domestically. After the legislation was signed into law on October 26, 2001, less than six weeks after 9/11, new reports began to

---

Services, 109th Cong. 2–7 (2005) (statement of Bradley E. Rock, American Bankers' Association, Chairman, President, CEO of Bank of Smithtown).

84. See JAEDICKE, supra note 80.

85. *Id.*

86. See Press Release, Office of Public Affairs, *Bush Administration Announces Creation of New Office in Ramped Up Effort to Fight the Financial War on Terror* (Mar. 8, 2004) (on file with author).

87. William J. Fox, Director Financial Crimes Enforcement Network, Address at United States House of Representatives: Subcommittee on Oversight and Investigations (June 16, 2004).

recite dollar amounts seized and frozen here and around the world, suggesting Patriot Act I had been the catalyst for America, through our banks, to win the war against terrorism.[88]

The problem is the BSA is just as ineffective against terrorism as it was against the war on drugs. Fox agrees, "the implementation of this risk-based regulatory system is a delicate matter that demands balance, consistency and clarity. The cornerstone of the Bank Secrecy Act, suspicious activity reporting, requires financial institutions to make judgment calls." He admits:

> If as regulators, we are too aggressive or too passive in supervising and examining the financial industries we regulate, there could be two equally unacceptable outcomes. Compliance should not be about second guessing individual judgment calls on whether a particular transaction is suspicious .... If on the other hand, we are too lax when it comes to ensuring institutions are implementing these programs, proper reporting will not be generated.[89]

Since BSA was first passed in 1970, the struggle to weigh an account holder's right to private bank records against legitimate government enforcement needs has been examined by the U.S. Supreme Court in several cases. Consistently since *Shultz*[90], the Supreme Court has held the Bank Secrecy Act constitutional stating that "the production by a bank of its records under subpoena is not as to the customer either a Fourth Amendment illegal search and seizure nor a Fifth Amendment self-incrimination."[91] However, from *Connally*, to *United States v. Miller*, and finally *United States v. Kaatz*[92], some major distinctions and vehement dissents occurred in District Court, the U.S. Court of Appeals for the Tenth Circuit, and the Supreme Court. Such a strong diversity of opinions merits a long overdue Supreme Court re-examination of this issue.

Connally made some clear distinctions about when a bank customer could reasonably expect some privacy concerning the details of his personal financial affairs. "[T]he District Court created at that time a requirement of a reasonable relationship between production of the bank reports and an invasion of a citizens right of privacy amounting to an unreasonable search within the meaning of the Fourth Amendment."[93] Citing the Supreme Court's decision in *Katz v. United States* and *Lewis v.*

---

88. Glenn R. Simpson, *U.S. Says al Qaeda Has Begun to Feel Financial Squeeze*, WALL ST. J., Nov. 15, 2001, at A28.

89. *Id.*

90. *Shultz*, 416 U.S. at 21.

91. *Connally*, 347 F. Supp. at 1248 .

92. United States v. Kaatz, 705 F.2d 1237 (10th Cir. 1983).

93. *See Connally*, 347 F. Supp. at 1245, 1246.

United States, the District Court said "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.[94] But what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected."[95]

In 1974, the Supreme Court went a step further. In dissenting, Justice Douglas recognized privacy in bank records:

> In a sense a person is defined by the checks he writes. By examining them, the agents get to know his doctors, lawyers, creditors, political allies, social connections, religious affiliation, educational interests, the papers and magazines he reads, and so on ad infinitum . . . It is I submit, sheer nonsense to agree with the Secretary that all bank records of every citizen "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." That is unadulterated nonsense unless we are to assume that every citizen is a crook, an assumption I cannot make.[96]

Justice Douglas also recognized that "[W]e only rush with the crowd when we vent on our banks and their customers the devastating and leveling requirements of the present [Bank Secrecy] Act. I am not yet ready to agree that America is so possessed with evil that we must level all constitutional barriers to give our civil authorities the tools to catch criminals."[97]

Of course, this was before we lived in fear, before the terrorist bombing on the World Trade Center on February 26, 1993; before the April 19, 1995 car bomb explosion in front of the Alfred P. Murrah Federal Building in Oklahoma City, Oklahoma that killed 168 along with 19 children;[98] well before the bombing of the United States embassies in Tanzania and Kenya, that killed 225 people on August 7, 1998; before the USS Cole was rammed by a suicide bomber on October 12, 2000 injuring 38 naval soldiers and killing 17;[99] before the horrifying loss of 2,992 lives on September 11, 2001;[100] and even before the terrorist bombings in

---

94. *See* Katz v. United States, 389 U.S. 347 (1967); Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559,563 (1927); *Connally* 347 F. Supp. at 1247.

95. *See* Rios v. United States, 364 U.S. 253 (1960); *Ex Parte* Jackson, 96 U.S. 727,733 (1877); *Connally*, 347 F. Supp. at 1247.

96. *See Shultz*, 416 U.S. at 85.

97. *Id.* at 86.

98. CNN Interactive, *Oklahoma City Tragedy: The Bombing*, *available at* http://www.cnn/com/US/9706/171McVeigh.overview.

99. *See* Howard Schneider & Roberto Suro, *Death Toll at 17 in USS Cole Blast; Some Doubt Yemenis Will Aid in Probe*, WASH. POST, Oct. 12, 2000, at A1.

100. Wikipedia: The Free Encyclopedia, http://en.wikipedia.org/wiki/casualties of the Sept. 11, 2001 attacks (stating that as of 2005, 2,992 people were presumed dead as a

Saudi Arabia and Morocco on May 20, 2003.[101] Yet, Douglas perceived the danger inherent in giving Big Brother his way.[102] In *Shultz*, Douglas remarked:

> Since Banking transactions of an individual give a fairly accurate account of his religion, ideology, opinions, and interests, a regulation impounding them and making them automatically available to all federal investigative agencies is a sledge-hammer approach to a problem only a delicate scalpel can manage. Where fundamental personal rights are involved–as is true when as here the government gets large access to one's beliefs, ideas, politics, religion, cultural concerns, and the like–the Act should be narrowly drawn.[103]

But by 1976, the fact that a bank depositor had no protected Fourth Amendment interest in domestic bank records maintained pursuant to the Bank Secrecy Act[104] was set in stone. Objections remained rampant, however, as evidenced by the strong dissents by Justice Brennan and Justice Marshall in *Miller*. Justice Brennan's dissent sharply criticizes the majority squarely on Fourth Amendment grounds. As Brennan pointed out:

> it cannot be gainsaid that the customer of a bank expects that the documents ... which he transmits to the bank in the course of his business operations, will remain private, and that such an expectation is reasonable ... Representatives of several banks testified at the suppression hearing that information in their possession regarding a customer's account is deemed by them to be confidential.[105]

Brennan continued with remarkable foresight when he exclaimed:

> For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account. In the course of such dealings, a depositor reveals many aspects of his personal affairs, opinion, habits and associations. Indeed, the totality of bank records provides a virtual current biography. While we are concerned in the present case only

---

result of all four Sept 11 attacks, including casualties at the World Trade Center, the Pentagon, on the airplanes, and the hijackers).

101. *See* Phillip Shenon, *U.S. Raises Terror Alert to Next Highest Level: Orange*, N.Y. TIMES, May 21, 2003, at A19.

102. *Shultz*, 416 U.S. at 85.

103. *Id.*

104. *Id.* at 435.

105. *Id.* at 449.

> with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to them by any police officer extends far beyond such statement to checks, savings, bonds, loan applications, loan guarantees and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential. To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.[106]

Brennan even foresaw the technology and trickery which the intelligence agencies would employ to accomplish the very deeds this dissent warns against:

> Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed. Development of photocopying machines, electronic computers, and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds.[107]

Brennan also warned against allowing access to bank account records without due process, saying "the potential for abuse is particularly acute where, as here, the legislative scheme permits access to this information without invocation of the judicial process."[108] This is exactly what Patriot Act I allows. Brennan concluded that in fact, there *is* a "reasonable expectation of privacy in the bank statements."[109]

Like his fellow justice, Marshall strongly warned against impinging upon Fourth Amendment protections. Because of his historical tours of litigation through the South during the 1950s and 60s, perhaps Marshall even foresaw the possibility of racial profiling. Whatever his motivations, Justice Marshall's legendary insight was clear in his dissent. Marshall dissents in *Miller* on the basis that the BSA was "a seizure of bank records within the meaning of the Fourth Amendment and unlawful in the ab-

106. *Id.* at 451.
107. *Id.* at 451,452.
108. *Id.* at 453.
109. *Id.* at 449.

sence of a warrant and probable cause."[110] His powerful words resonate loudly considering our current situation: "I wash my hands of today's extended redundancy by the Court. Because the recordkeeping requirements of the Act order the seizure of customers' bank records without a warrant and probable cause, I believe the Act is unconstitutional."[111]

By the time *Kaatz* was decided in 1983 there was no moving the Supreme Court from the position it had supported in *Connally* and *Miller*. A Fifth Amendment discussion had also entered the scene. Although *Kaatz* concerned a CTR as opposed to the production of a check, as in *Connally*, the ruling in *Kaatz* remains applicable.[112]

Kaatz speaks directly to the question of whether a bank filing a CTR with the IRS, pursuant to the BSA, is in contravention of a customer's Fourth Amendment rights, and whether notice to the account holder of such a filing is required. The U.S. Court of Appeals for the Tenth Circuit, applying the law in *Connally*, decided there was neither a violation of the Fourth Amendment by the filing of the CTR, nor the failure of the bank to give notice to Kaatz, its customer, that the CTR was executed by the bank and sent to the IRS voluntarily.[113] "The customer had no legitimate 'expectation of privacy' concerning information contained in bank records."[114] Quoting the 1974 Supreme Court decision in *Shultz*, the *Kaatz* court found "the regulations do not require the banks to notify the customer of the report . . . . and the banks are left free to adopt whatever customer notification procedures they desire." As to the Fifth Amendment argument Kaatz asserted, the Court replied "the Fifth Amendment is limited to 'prohibiting the use of physical or moral compulsion' exerted on the person asserting the privilege. [Morton] was not forced to buy the certificate of deposit or to use currency in doing so. No compulsion was exercised on the defendant and no right of privacy existed within the protection of the Fifth Amendment."[115]

While the terrorist events of 2001 and the current climate of banking demand balanced consideration, it is important to note that courts once found Fourth Amendment rights so much at the core of American values, that they refused such an encroachment. The District Court for the Northern District of California understood and articulated this as early as 1972 in *Connally*:

---

110. *Id.* at 455.

111. *Id.* at 456.

112. *Kaatz*, 705 F.2d at 1241–42.

113. *Id.*

114. See *id.* at 1242; *Miller*, 425 U.S. at 442.

115. *Kaatz*, 705 F.2d at 1242; see also Fisher v. United States, 425 U.S. 391, 397 (1976).

> The Act [BSA], insofar as it authorizes the Secretary to require virtually unlimited reporting from banks and their customers .... as a surveillance device for the alleged purpose of discovering possible, but unspecified, wrongdoing among the citizenry, transcends the constitutional limits ... as to unreasonably invade the right of privacy protected by The Bill of Rights, particularly the Fourth Amendment provision protecting the right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures.[116]

The entire position of the Supreme Court built upon *Connally* must then be re-examined in light of Patriot Act I. There is real inconsistency where the United States Court of Appeals for the Tenth Circuit says on the one hand that Kaatz had no Fourth Amendment right to his account information while on the other hand, the United States District Court for the Northern District of California made it plain in *Connally* that the BSA "insofar as it authorizes reporting from banks as a surveillance device ... transcends the constitutional limits as laid down by the United States Supreme Court."[117] The United States Supreme Court *should find* a Fourth Amendment right of privacy in our bank records. Since we require probable cause in all other private aspects of American life, it would be unconstitutional *not* to protect the financial records and activities of Americans.

This seems especially true considering that financial records have been proven to be only minimally useful in detecting terrorism. "[T]he relatively small amounts of money required for terrorist acts can easily pass unnoticed."[118] Certainly there have been a few instances in which money wires are connected to questionable Muslim charitable organizations, even organizations identified as contributing to Al Qaeda causes. These discoveries have been minute. In most instances, financial records are being used as a springboard to get into the private information of an individual's life, even if this initial information is irrelevant to terrorism. Very few individuals[119] whose bank accounts have been probed are actually connected to terrorist activities. Not only must the right to privacy in financial records be given constitutionally protected status, it is a right that is easy to administer. Like all other areas of constitutionally protected American life, if the Court granted bank records Fourth Amendment protection, all that would be required of government intelligence agencies to

---

116. *Connally*, 347 F. Supp. at 1251.

117. *Id.* at 1251.

118. ALFRED B. PRADOS & CHRISTOPHER M. BLANCHARD, CRS REPORT FOR CONGRESS, SAUDI ARABIA: TERRORIST FINANCING ISSUES 1 (2004)(on file with author).

119. *See* FINANCIAL CRIMES ENFORCEMENT NETWORK, DEP'T OF THE TREASURY, FINCEN's 314(a) FACT SHEET, http://www.fincen.gov/314afactsheet.pdf.

secure bank account access is probable cause that a crime had or will be committed.

If there is sound reasoning, there is probable cause, and a warrant is issued, a probe is authorized, the evidence is allowed, the subversion is discovered, the terrorist activity is exposed. By this procedure, government agencies will have no problem finding the relevant evidence. What could possibly be wrong in continuing the established procedure to overcome American privacy rights when securing government access to a citizen's information? Furthermore, if Americans claim not to tolerate indiscriminate bias against any American citizen, then we must uphold that promise to all Americans, Muslim, Middle Eastern, and "Middle Eastern-looking" Americans alike.

IV. CONSTITUTIONAL CONSTRAINTS AND IMPLICATIONS OF EXISTING BANK POLICIES

> *The problem is not just racial profiling in the criminal justice system. It's racial profiling in life.*[120]

Banks have a great deal of discretion within their specific policy guidelines as to whom they monitor and report to FinCen. The challenge for banks is to decide responsibly who to monitor. During this time when the liberties of all Americans are threatened, banks should be especially vigilant to treat all account holders with similar respect. Can banks, within the actual guidelines of their operating policies, specifically target those who "appear Middle Eastern?" On their face, do the Know-Your-Customer Bank policies allow for this possibility? Do banks really use racial identity alone to identify someone as a suspicious account holder? The central question however is: Is targeting or monitoring an account holder's activity strictly based on that holder's ethnicity or perceived ethnicity an invasion of constitutionally protected privacy rights? *Who* is doing the profiling is an important part of the analysis. While we have a certain set of Constitutional protections from law enforcement we have no comparable rights given to us from bank employed individuals, who clumsily identify possible terrorist activity and hence file CTRs or SARs. In fact, the head of FinCEN has actually said that the decision to report often comes down to a "hunch."[121] A citizen's privacy rights are

120. Hazel Trice Edney, *Candidates Sharply Contrast on Race Issue*, DISTRICT CHRON., July 22, 2002, at Cover.

121. *See* Patti Waldmeir, *Inside Track-Unaccustomed Warriors—A New Law in the U.S. Will Draft Thousands of Businesses Into the Fight Against Terrorism*, FIN. TIMES, Mar. 21, 2002, at 17.

demolished by bank employees who are themselves protected from civil repercussions for their mistakes.[122]

Correct compliance with SAR and CTR requirements dictated by the Department of Treasury is arguably straightforward, but not extremely rigid. Most banks issue internal on-line detailed instructions to guide its employees to correctly comply. Almost every Bank's policy is a keyboard stroke away from the bank personnel who need more instruction.

A. *Have the Bank Policies Created in Response to Patriot Act I Strengthened National Security?*

Appropriate or not, banks are trying to avoid liability from under-reporting. They are struggling with how to detect fraud, money laundering, and terrorist activity without violating procedural norms. Banks understand how precarious the balancing act is between protecting account holder privacy and national security. Although there is no question that reporting can be an effective tool in the war against terrorism, the question is, *how* effective of a deterrent the reporting devices have been and can be. The truth is CTRs and SARs have limited abilities to detect criminal behavior, thereby defeating their viability.

Another burden that banks face is the time and expenses associated with reporting:[123]

---

122. Annunzio-Wylie Anti-Money Laundering Act, Pub. L. No. 550, 106 Stat. 4044 (1992) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., 31 U.S.C., and 42 U.S.C.) (holding banks free from liability for reporting suspicious activity). The safe harbor in the BSA protects banks from liability for three types of disclosure:

1) A disclosure of any possible violation of law or regulation.
2) A disclosure pursuant to 31 U.S.C. § 5318(g)(3).
3) A disclosure pursuant to any other authority. *See infra.*

Pursuant to *Lee v. Bankers Trust Co.:*

> [T]he safe harbor provision applies regardless of whether the SAR is filed as required by the Act or an excess of caution . . . The plain language of the safe harbor provision describes an unqualified privilege, never mentioning good faith . . . broadly and unambiguously provid[ing] for immunity from any law (except the federal Constitution) for any statement made in [a] SAR by anyone connected to a financial institution.

Lee v. Bankers Trust Co., 166 F.3d 544 (2d Cir. 1999)(emphasis added). *See also* Stoutt v. Banco Popular, 320 F.3d 26, 31–33 (1st Cir. 2003) (finding that immunity is granted to any financial institution that discloses "any possible violation of law," regardless of whether the lender had good faith belief); Brown v. Nationsbank Corp., 188 F.3d 579, 589 (5th Cir. 1999) (stating that "if private businesses were not eligible for immunity from . . . claims arising from assisting undercover federal operations, this would provide a major disincentive to assisting law enforcement and would undermine the needs and interests of the federal government."); Lopez v. First Union Nat'l Bank of Fla., 129 F.3d 1186, (11th Cir.1997), aff'd by Whitney Nat'l Bank v. Karam, 306 F. Supp. 2d 678 (S.D.Tex. 2004).

123. During the past 25 years, the compliance burden has grown so large and is so pervasive throughout all levels of bank management that it is extremely difficult to measure. Research done by the ABA and the Federal Reserve indicates that the total cost of compli-

> The current regulatory environment is having a negative effect on financial institutions and the economy in general. U.S. financial institutions will spend $10.9 billion through 2005 on AML [Anti-Money Laundering] compliance alone. $695 million will be spent on software and hardware, $3.3 billion for information systems maintenance and the rest of the costs will be allocated toward employee training, reporting, and other compliance costs.[124]

The financial burdens and constitutional infringements seem to clearly outweigh the possibility of terrorist detection. And even with these burdens and infringements banks cannot detect every potential terrorist or dollar being used to fund terrorist activities.

FinCEN publishes reports of success stories[125] that include what information in a particular CTR or SAR led to a positive enforcement action. Unfortunately, this practice rarely exposes the particular information in the BSA reporting process which led to the discovery of a violation. As a result, this fails to give banks any extra guidance about what information they should be reporting. Furthermore, the reporting occurs over such an extended period of time that when a "BSA guidance" story is highlighted by FinCEN it leaves no clear trail as to what information the bank(s) reported which proved instrumental to the success of the operation.[126] FinCEN however does maintain a "Quick Reference Guide for Money Service Businesses on Reporting Suspicious Activity" on its website which points out a "number of possible factors, or 'red flags'

---

ance *today* for banks would range from $34 billion to $42 billion per year and this does not include compliance costs due to legislation such as the USA Patriot Act. For the typical small bank, about one out of every four dollars of operating expense goes to pay the costs of government regulation. For large banks as a group, total compliance costs run into the billions of dollars annually. *See* Statement of Bradley E. Rock, *supra* note 83, at 4–5.

124. Comment Letter to the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, from Richard M. Whiting, Executive Director and General Counsel of The Financial Services Roundtable, May 4, 2005 p.6 (on file with author).

125. *See* Law Enforcement Cases Supported by BSA Filing, *at* http://www.fincen.gov/le_casesdetail.html.

126. *See* Financial Crimes Enforcement Network, Dep't of the Treasury, *Numerous SARs and CTRs Aid in Hawala Investigation*, www.fincen.gov/hawalainvestigation.html (providing no guidance as to what information was reported by banks or what led the banks involved to file a SAR, but indicating that the FBI only opened their investigation and queried the BSA database into the activities of the dealer after receiving a citizen complaint); Financial Crimes Enforcement Network, Dep't of the Treasury, *Decade Long Investigation from Bank's Filing of Suspicious CTRs Leads to Convictions*, http://www.fincen.gov/suspiciousctrs.html (providing only slightly more direction for banks concerning the filing of a SAR).

which signal an activity or transaction that might be suspicious."[127] The reference guide suggests that bank employees ask themselves questions such as "[i]s the amount of the transaction unusually large for the typical customer or for the money service business? Does the customer make similar transactions more frequently than normal? Does the transaction seem unusual for the customer?" The guide gives examples such as:

> customer uses fake ID, two or more customers use similar IDs, customer changes a transaction after learning that he or she must show ID, two or more customers seem to be working together to change the transaction to evade BSA by structuring, breaking up transactions, using two or more bank or money service locations on the same day.[128]

The guide continues, "if a customer offers a bribe or admits to a crime the law requires you to file a SAR if it involves or aggregates funds or other assets of $2,000 or more."[129] Clearly, the decision to report or not to report is governed by selection standards determined entirely by law enforcement.

Bankers argue validly that whether a bank follows the FinCEN Guide or it gleans from other available data what should be reported as suspicious, there is no inerrable system of distinguishing terrorists from the benign account holder. This makes the possibility that an innocent account holder would be subject to an illegal search and seizure, and highlights the reasons for strengthening the protections against such an illegality. The Supreme Court should establish the Fourth Amendment right to privacy in every American bank account. As long as this precursor to monitor a bank account or transaction exists, the bank or the intelligence agency using the SAR or CTR is able to justify its intervention into the privacy of every American citizen, irrespective of what the initial catalyst was for the bank's or government's intrusion.

B. *Constitutional Consequences of the Homeland Security Act*

The Homeland Security Act establishes a central agency that accesses, receives, and analyzes intelligence information, law enforcement information, and any other information from federal, state and local agencies, even from the private sector, in an attempt to promote security in America.[130] Critical infrastructure information (sought voluntarily from the private sector) is used in conjunction with known government intel-

127. FinCen, *Reporting Suspicious Activity: Quick Reference Guide for MSBs*, http://www.fincen.gov/reg_guidance.html.

128. *Id.*

129. *Id.*

130. *See* USA Patriot Act § 201.

ligence to implement protected systems analysis, a national warning system, interdependency studies, recovery and reconstitution methods. As long as information is submitted to Homeland Security in good faith, it will not be disclosed or used in any civil action arising under state or federal law.[131] However, all information Homeland Security receives is not submitted in good faith.

The public is largely unaware of Homeland Security action until they, are or one of their business relationships, are affected. Blacklisting and Brownlisting are no longer only foreign policy or political tools, they are being used as justifications to conduct acts of criminal secret civil rights infringement.

The primary objection to the Homeland Security Act is that it is yet another governmental agency with access to both law enforcement data and the private information of Americans. Additionally, the Act synthesizes information gathered from the private sector to evaluate the level of security risk an individual poses, irrespective of the trust-worthiness of that information. Neighbors, co-workers, and anyone one associates with who offers information to this agency , whether that information be truth or fabrication, can be combined with legally or illegally obtained information by the government to determine whether that individual constitutes a security risk. This poses an obvious danger for Muslim citizens or citizens of Middle Eastern descent. The consequences of these lists have created many problems, only one of which is financial discrimination. Under this Act, informing, investigation and final finger-pointing are all done in secret. The byproducts are account closures, halted wire transfers, and even credit withdrawal for Americans. Any American is fair game, but increasingly the civil rights of Saudi-, Arab-, Iraqi-, and Muslim-*Americans* have suffered.

V. THE PROBLEM LEGISLATION
THE USA PATRIOT ACT: THE FIRST LEGISLATIVE RESPONSE TO THE EVENTS OF SEPTEMBER 11, 2001

Legislative interpretation of the 342-page Patriot Act I created quite a bit of chaos in the financial industry. The Senate sent the Patriot Act directly to the floor without debate or opportunity for analysis on the 350 different subject matters and forty agencies[132] it would impact. The Act was passed less than six weeks after the initial proposal by the Financial Action Task Force and the September 11 attack on the World Trade

131. *See id.* at §§ 212–14.

132. *See generally, id.* at §§ 1–1016; Editorial, *Infringing on Civil Liberties,* ST. PETERSBURG TIMES, Oct. 29, 2001, at 10A (approved by a margin of 356 to 66 by the House of Representatives and 98 to 1 by the Senate); J.M. Lawrence, *War on Terrorism; Anti-Terror Laws in Place; Feds Urgently Implement Crackdown,* BOSTON HERALD, Oct. 27, 2001, at 5.

Center. Any conflicts which arose were settled through private conversations between the Justice Department and party leaders. "The Bush administration implied that members who voted against it would be blamed for any further attacks –a powerful threat at a time when the nation was expecting a second attack to come any moment and when reports of new anthrax letters were appearing daily."[133] It becomes simple to see the "triangle of fear"[134] used to influence the Senate and the American people that Patriot Act I would be a sound response to the perhaps tenuous need to monitor the flow of cash through our nation's banks, lest some of that cash be channeled into fuel for terrorist activities.

Many suspect Patriot Act I of being developed in the shadows of the government long before the 9/11 terrorist attack. While the Act passed with overwhelming support, there were multifarious concerns echoing in the halls of Congress about how to control the potential loss of privacy and the feared abuses of power. Even now, the Congressional intent of many of the provisions and compliance requirements remain unclear. Patriot Act I has not been entirely well received by any group outside of law enforcement. Human rights, civil rights, policy review, and city councils across the nation all object to the expansiveness of the Act. On May 29, 2003, Philadelphia, the fifth largest city and birthplace of the U.S. Constitution and the Declaration of Independence, became the 117th state or local government to approve measures opposing the Patriot Act as a threat to the Constitutional rights of citizens. The resolution, passed by the City Council, called for members of Congress to work for the repeal of the federal legislation which granted the Justice Department broad new police powers.[135]

As established, financial institutions are protected from privacy lawsuits under Patriot Act I and the Annunzio-Wyle Anti-Money Laundering Act. Yet no one knows the extent to which Patriot Act I has infringed on the Constitutional rights and protections pursuant to the Fourth Amendment.

The aggressiveness of the Patriot Act I creates several important Constitutional issues for banks and bank employees:

Fourth Amendment—Patriot Act I increases government surveillance powers by allowing warrantless searches of account holders' lives, activities

133. American Civil Liberties Union, *Surveillance Under the USA Patriot Act*, http://www.aclu.org/safefree/general/17326res20030403.htm.

134. CHRISTOPHER SCHEER ET AL., THE FIVE BIGGEST LIES BUSH TOLD US ABOUT IRAQ 37 (2003) (explaining the term "triangle of fear" as referring to the linking [of] Iraq's megalomaniacal dictator, Saddam Hussein, to both a vast arsenal of weapons of mass destruction he was alleged to possess and to the terrorist organization Al Qaeda, believed to be behind the 9/11 massacre).

135. *Philadelphia Panel Spurns Patriot Act*, THE SAN DIEGO UNION-TRIB., May 30, 2003, at A7.

and habits memorialized in bank records in violation of the Fourth Amendment requirement to show probable cause.

Fourth and First Amendment—The Fourth Amendment is also affected by the increased searches of "foreign intelligence information" and "trap and trace" searches using computers to deduce the origin and/or destination of communications, wires, etc. This has various negative effects on banking relationships with foreign banks. It also violates the First Amendment by permitting an investigation solely based on an individual's exercise of his right to freedom of association.

Fifth and First Amendment—In direct violation of the Fifth Amendment Due Process clause, Patriot Act I allows government invasion into private bank records, without notice to the affected individuals, thereby circumventing RFPA. Bank employees receiving search orders or generating reports required by the BSA, are restricted by Patriot Act I from disclosing the existence of that order or report to the account holder or anyone outside the proper government agency. This could also violate the constitutional right to free speech guaranteed by the First Amendment if a bank employee is prohibited from disclosing that they have been served with a search order, regardless of whether there is a need for concealment.

For the first time, under Patriot Act I, a wider segment of the financial industry was responsible for reporting under the Act, due to the redefinition of "financial institution." Institutions such as brokerage houses, money service businesses, casinos, and real estate companies became responsible for first drafting and then complying with an anti-money laundering and terrorist identification scheme. Clearly, uncovering and preventing access to terrorist financing is of grave importance. However we know little about this (as evidenced by the five pages devoted to discussion of funding for the 9/11 attack by the National Commission on Terrorist Attacks in its official report),[136] and are able to control less, the manner in which Al Qaeda and other terrorist groups are funded.

---

136. The 9/11 Commission estimates between $400,000 and $500,000 was spent to plan and conduct the attack. According to the CIA, it was al Qaeda-funded with "about $30 million per year to sustain its activities before 9/11 and that this money was raised almost entirely through donations." The money was moved, stored and spent in ordinary ways easily defeating the detection mechanisms in place. The origin of the funds remains unknown. Bin Laden inherited approximately $300 million when his father died, kept his assets in Sudan and received about $1 million per year from this fortune. Bin Laden drew on ties to wealthy Saudi individuals, relied on a core group of financiers who raised money from donors in primarily Gulf countries and Saudi Arabia, gathered Taliban financial support when he was in Afghanistan, collected money from employees of corrupt charities, and the al Wafa organization may have funneled money to al Qaeda who had access to al Wafa bank accounts. Al Qaeda has been alleged to have used a variety of illegitimate means, particularly drug trafficking and conflict diamonds, to finance itself. Ultimately, the U.S. government has not been able to determine the origin of the money used for the 9/11 attacks. *See* NAT'L COMM'N ON TERRORIST ATTACKS IN THE U.S., THE 9/11 COMMISSION REPORT 169–172 (2004) (finding that al Qaeda has been alleged to have used a variety of illegitimate means, particularly drug trafficking, to finance itself.

There has been *some* due diligence in identifying the source of funds for the 9/11 terrorist attacks. The plaintiffs in *Burnett v. Al Baraka Investment* brought suit against all "persons and entities that funded and supported the international terrorist organization known as Al Qaeda, which . . . carried out the attacks,"[137] identifying Al Rajhi

> as the largest retail bank in Saudi Arabia. Plaintiffs central allegation against Al Rajhi is that [the banks] have acted as instruments of terror, in raising, facilitating and transferring money to terrorist organizations. [The allegation also is that] Al Rajhi is the primary bank for a number of charities that serve as al Qaeda front groups . . . .[138]

The same problem arises when dealing with American banks, in that there is no obvious direct link from American banks to terrorist organizations like Al Qaeda. The United States District Court for the District of Columbia responded to Plaintiffs' allegation by saying that:

> [t]he act of providing material support to terrorists, or 'funneling' money through banks for terrorists is unlawful and actionable—but again—Al Rajhi is alleged only to be the funnel. Plaintiffs offer no support, and we have found none, for the proposition that a bank is liable for injuries done with money that passes through its hands in the form of deposits, withdrawals, check clearing services, or any other routine banking service.[139]

Although it seems reasonable to hold banks liable for actively shielding terrorist funds, they must not use racial profiling as a means to identify potential terrorists and reduce their responsibility to conduct adequate research.

While Patriot Act I gives government agencies and banks enhanced investigative techniques to pinpoint terrorist targets, it heightens the obvious pitfalls of racial profiling. Although it has been partially responsible for capturing $34 million dollars[140] linked to terrorism, and while it also

---

Ultimately the U.S. government has not been able to determine the origin of the money used for the 9/11 attacks). *See also* Douglas Farah, *U.S. Saudi Anti-Terror Operation Planned; Task Force Will Target Funding*, WASH. POST, Aug. 26, 2003, at A1 (reporting that intelligence experts say that funding from wealthy individuals on the Arabian Peninsula, principally Saudi Arabia, to al Qaeda still amounts to millions of dollars a year); SCHEER ET AL., *supra* note 134, at 39.

137. Burnett v. Al Baraka Inv. and Dev. Corp., 274 F. Supp. 2d 86, 91 (D.D.C. 2003).

138. *Id.* at 109.

139. *Id.*

140. *The Financial War on Terrorism: New Money Trails Present Fresh Challenges, Hearing Before the S. Comm. on Finance*, 107th Cong. 3 (2002) (statement of James Gurule, Undersecretary for Enforcement).

has the potential to serve as a deterrent, its effects since its initial inception has been marginal. The governmental agencies using these enhanced surveillance methods must constitutionally justify the Act's effectiveness to Congress, the American people, and courts, the tenets of our justice system. Our Constitution demands this.[141]

VI. BUILDING ON FLAWS: THE PROPOSED DOMESTIC SECURITY ENHANCEMENT ACT—PATRIOT ACT II

> *"The Fourth Amendment creates "zones of privacy" which protect against governmental invasions of the . . . privacies of life . . . ."*[142]

Increasingly the term "racial profiling" has arisen in the forum of public debate in reference to government activity directed at individuals because of their race. There is no denying the events of September 11 caused law enforcement to focus upon Muslims, foreign nationals of Middle Eastern descent, and those who "appear to be of Middle Eastern descent." However, not only is discrimination in America against the law and our sense of fairness, it undermines the melting pot ideal on which America was founded. Our national principles and the U.S. Constitution require a conscious determination of whether using profiling based on race in this context and any success in apprehending terrorists using these methods merits a continuation of the suspension of Fourth Amendment and First Amendment principles. Certainly, federal officials must create tools to combat terror carried out by terrorists. However, that cannot be accomplished by abolishing the building blocks of democracy. Like Patriot Act I, Patriot Act II as drafted by the staff of Attorney General John Ashcroft[143] accelerates the serious erosion of Constitutional rights.

Several specific provisions of Patriot Act II[144] have drawn significant objections:

Under Sections 102–109, 120–122 and 124: Concerning wiretaps and Surveillance, there would be no limits on what police could examine in the areas of religious and political activity. Credit records and library records become freely available without a judicially justified warrant, and any organization identified as involved in any form of civil disobedience

---

141. U.S. CONST. amend. I, IV.

142. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (citing Boyd v. United States, 116 U.S. 616,630 (1885)).

143. Charles Lewis & Adam Mayle, *Justice Department Drafts Sweeping Expansion of Anti-Terrorism Act,* THE CENTER FOR PUBLIC INTEGRITY, Feb. 7, 2003, http://www.publicintegrity.org/report.aspx?aid=94.

144. American Civil Liberties Union, *Interested Persons Memo: Section-by-Section Analysis of Justice Department draft "Domestic Security Enhancement Act of 2003" also known as "Patriot Act II," Feb. 14, 2003,* http://www.aclu.org/safefree/general/17203leg20030214.html.

would be open to wiretapping. Wiretaps under Patriot Act II can be accomplished without a court order for 15 days after any terrorist attack.

Sections 125–129 These sections propose "national security letters" which resemble administrative subpoenas that intelligence and other government agencies can use to obtain and utilize information in national security investigations. These sections significantly strengthen the government's access to travel records, financial records, and all types of consumer reports, including consumer credit reports. They also authorize the Justice Department to eavesdrop on or conduct furtive searches of any suspected terrorist or foreign agent for 15 days after a military conflict or a declaration of war.

No objection to spying on the "type" of people we are eager to classify as terrorists? The problem is, these Sections can focus the government's intrusiveness onto American citizens. The ability of the government to initiate wiretaps on U.S. citizens for a greater length of time and with less court involvement is enhanced if terrorism is made the subject of investigation. Surveillance of an American citizen suspected of spying for a foreign power is allowed, even when the activity alleged to be "suspicious" conduct is not in fact criminal. An even more dangerous problem is that under these sections, the Attorney General would no longer have to personally authorize the use of certain intelligence evidence in criminal cases, he could simply delegate this responsibility.

Under Section 501: "Expatriation of Terrorists," an American supporter who becomes a member of, or provides material support to, a group engaged in civil disobedience could lose his citizenship. A citizen normally has to *denounce* his citizenship; however, under this section his intent can be inferred from conduct.

Patriot Act II undermines the very essence of our criminal justice system by allowing these actions at all, but it is especially troublesome when these activities are conducted secretly. Proposed Patriot Act II bypasses Congress by permitting foreign initiated searches and wiretaps without the requisite treaty permission. Patriot Act II would eliminate our federal checks and balances by destroying the constitutional limits imposed on wiretaps, access to confidential records, police power searches and surveillance, and government spying on religious and political expression. Surely it is obvious that while Patriot Act II purports to establish more power to subdue terrorists, it actually empowers our government to use these tools on American citizens who have no connection with terrorist activities. The ACLU points to RICO and suggests that when the:

> Racketeer Influenced and Corrupt Organizations Act was enacted by Congress, Congress intended those extraordinary powers to be used against the Mafia and organized crime. Over the years, however, RICO was used far more broadly, even against anti-abortion protestors and other dissidents. The sug-

> gestion is that some of the powers the government may be seeking in Patriot Act II, while ostensibly directed at terrorists, could likewise be used in unexpected ways.[145]

Patriot Act II means more government intrusion, more constitutional infringement, more threats to American citizenship, and less safeguards on federal intelligence and law enforcement. Enacting this legislation would magnify the egregious mistakes made in Patriot Act I.

CONCLUSION : THE BALANCING ACT

> *"They that can give up essential liberties to obtain a little temporary safety deserve neither liberty nor safety."*[146]

Does Patriot Act I allow banks to identify terrorists, and hence strengthen national security, without compromising the constitutionally protected privacy of account holders?

> The Patriot Act is unprecedented in its amendment to provisions that had previously checked the ability of the government to observe everyday activities and obtain personal information about citizens. The fact that it does so in such a potentially oppressive manner has not quite hit consciousness of the American people. Privacy in the sense of freedom from government intrusion, is a necessary foundation for the free exercise of democracy.[147]

Patriot Act I, and proposed Patriot Act II, are dangerous legislative tools that are too vague and unproven to prevent terrorism. We must not be asked to give up our Constitutional right to privacy in a desperate attempt to sniff out the terrorists who pass in and out of our banking system. As the "American death toll in Iraq reaches 1,594, and the wounded exceed 10,000"[148] we must consider what the lives of our sons and daughters, mothers and fathers, sisters and brothers mean. Americans like to say our troops are dying for freedom, but does that include freedom in our banking lives? It seems that how Americans spend their

---

145. American Civil Liberties Union, *How "Patriot 2" Would Further Erode the Basic Checks on Government Power That Keep America Safe and Free*, Mar. 20, 2003, http://www.aclu.org/safefree/general/17346leg20030320.html (quoting Scheidler v. Nat'l Org. for Women, Inc., 537 U.S. 393 (2003)).

146. THE ELECTRIC BEN FRANKLIN, http://www.ushistory.org/franklin/quotable/quote04.htm.

147. *See* Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act*, 80 DENV. U. L. REV. 375, 378–79 (2002).

148. Charley Reese, *Two Years Out*, LEWROCKWELL, May 9, 2005, http://www.lewrockwell.com/reese/192.html.

money and who has access to this information, is at the root of that freedom.

Patriot Act I was an emotional lapse of judgment on the part of the Senators who, save but one,[149] voted to pass it. Members of both the House and the Senate had concerns about the potential intelligence abuse of power by government intelligence and the resulting loss of privacy for Americans.[150] Before USA Patriot Act was even conceived, our government intelligence agencies were covertly doing all Patriot Act I purports to do. Patriot Act II is beyond the powers any citizen of common intelligence would believe necessary to combat terrorism.

Under Patriot Act I, identifying potential terrorists has become dangerously close to racial profiling. We already have rogue police officers, who use any excuse, racial profiling included, to haul Black and Brown people over to the side of the road, search their cars, arrest and fingerprint them. Patriot Act I allows him, while the victim is in the station posting bail, to secure a warrant and search the victim's home based on what he may find in a person of color's vehicle. So what is to stop the rogue officer from securing your DNA using proposed Patriot Act II, Section 301–606, wiretapping your telephone, and hijacking your bank account records? Certainly not Patriot Act I and II. As a young girl preparing for the National Spelling Bee, I thought I had to learn words like antidisestablishmentarianism. Who would have known I would live to see a climate in America where government agencies wish for such a state. Americans are being forced by this legislation to compromise our Fourth Amendment rights. In return, the government has found few money trails in American banks that expose terrorists. Thus Americans have gained little, in return for giving up much.

At the policy level, banks have written SAR, CTR and "Know-Your-Customer" policies that reasonably disallow for discrimination. While there is some language in the bank policies which raises concerns, for the most part it is unintended, perhaps even the product of poor technical writing. Unfortunately, the language in the policies permit bank employees' discretion. Remember, these are the people who see and interact with "the customer," and therefore this is the level where discrimination is most likely to occur.

During an in-person transaction, the possibility for discrimination remains, on the basis of a Middle Eastern surname, or using visual ethnic identity. It must be clear to those who deal with banks account holders

149. Democrat Russell Feingold of Wisconsin was the only senator who voted against the USA Patriot Act in 2001. Only 66 representatives voted against the USA Patriot Act (implying that only Feingold was concerned about government abuse and privacy loss, although others felt pressured to vote for it).

150. Robert E. Pierre, *Wisconsin Senator Emerges as a Maverick: Feingold, Who Did Not Back Anti-Terrorism Bill, Says He Just Votes His Conscience*, WASH. POST, Oct. 27, 2001, at A8.

that characteristics like ethnic identity are not valid, and that *behavior* is the key to identify a terrorist.

The people charged with implementing Patriot Act I in banks are human and human judgments are often weak and inherently flawed. The problem for banks and other financial institutions will always be the tendency of employees to rush to judgment in applying the policies. Given this weakness, the most effective way to detect terrorists' money in banks is via the legislation itself. Patriot Act I, its ineffectiveness, its implications on the First, Fourth, and Fifth Amendments of our Constitution, and its safe harbor provision which protects bank personnel from their overt or covert discrimination, is the real source of discrimination.

Patriot Act II is a step that only magnifies this outrage, and one which must not be taken. The war on terrorism makes racial profiling seem legitimate, even necessary. But, it does not take much imagination to see what continuing Patriot Act I beyond 2006 or implementing Patriot Act II would do.

Already, a bipartisan group of Representatives and Senators are proposing the "End Racial Profiling Act."[151] This legislation contains a number of methods to both identify when profiling occurs and create provisions that attempt to stop this racial, ethnic, religious and national origin profiling. Almost half of the states have passed similar legislation. ERPA is designed to pick up where the 2003 Department of Justice's guidelines prohibiting racial profiling ended. It creates a long overdue cause of action for victims of racial profiling. Aside from Johnny Cochran's success in the New Jersey racial profiling cases,[152] victims of racial profiling have never found much justice in the courts. ERPA requires a national uniform data collection system to promote police accountability. One of the proposed measures allows funds to be withheld by the attorney general from police departments which continue behavior that resembles racial profiling or refuse to comply with the directives of ERPA. So that there can be no valid excuse not to comply, ERPA provides grants to assist police agencies to collect the necessary racial profiling data. Already, over 100 members of Congress and many public advocacy groups—including progressive law enforcement organizations—have joined to co-sponsor the Act.[153]

The U.S. Department of Justice has also responded to profiling in the context of law enforcement in November of 2000 by creating *A*

---

151. End Racial Profiling Act of 2004, H.R. 3847, 108th Cong. (2004); End Racial Profiling Act of 2004, S.2132, 108th Cong. (2004) (sponsored by Reps. John Conyers, D-MI and Christopher Shays, R-CT in the House of Representatives and introduced in the Senate by Senator Russ Feingold, D-WI, with support of 128 members of the House and 16 members of the Senate for ERPA).

152. *See* JOHNNIE COCHRAN, A LAWYER'S LIFE 209–30 (2002).

153. End Racial Profiling Act of 2004, H.R. 3847, 108th Cong. (2004); End Racial Profiling Act of 2004, S.2132, 108th Cong. (2004).

Resource Guide on Racial Profiling Data Collection Systems.[154] Racism is a disease we must be committed to defeat. Profiling has not enhanced national security; not a single arrest, not a single dollar found by a SAR or CTR report since the aftermath of 9/11, has been traced to a terrorist act. Moreover, the Treasury Department is now so overwhelmed by the sheer number of SARs and CTRs, if there were evidence of terrorism uncovered by these devices, it would be months before the particular SAR would be identified.

A. *Proposals for Solution*

Instead of taking more Constitutional liberties of the American people, the unbridled issues which arise under Patriot Act I and now Patriot Act II, should be addressed. Here are several proposed directives:

Rather than debate the merits of The Patriot Act, Congress must examine whether it has secured results. Not a single terrorist has been discovered by using the dual CTR and SAR reporting devices. It was entirely unreasonable to reenact portions of Patriot Act I when it became due for examination in 2005. As an alternative to re-enactment, Patriot Act I should be limited in its application to terrorists or only the people on the various government intelligence agency watch lists. If Patriot Act I is limited to veritable instances of terrorism there will be minimal objection to its advocacy of increased surveillance ability (including everything from wiretapping, pen registers, trap and trace and record keeping to monitoring physical movements, financial institution reporting, search span) by the expanded roles of the CIA, FBI, DOJ, and the Treasury Department.

As the 9/11 Commission has advocated,[155] appoint one neutral leader over terrorism as head of the National Counter Terrorism Center, whose

---

154. RAMIREZ ET AL., *supra* note 2, at iii (urging more jurisdictions to determine whether discriminatory policing existed in the area through voluntary data collection efforts. This guide was prepared by Northeastern University with funding from the U.S. Department of Justice after President Clinton and U.S. Attorney General Janet Reno, civil rights leaders, police and government leaders convened in Washington D.C. at the conference *Strengthening Police-Community Relationships* June 8–9,1999, and provides an overview of the nature of racial profiling; a description of data collection and its purpose; current activities in California, New Jersey, North Carolina, and Great Britain; and recommendations for the future).

155. THE 9/11 COMMISSION REPORT, *supra* note 136, at 403, 405. Stating:

> We recommend the establishment of a National Counterterrorism Center (NCTC), built on the foundation of the existing Terrorist Threat Integration Center (TTIC). Breaking the older mold of national government organization, this NCTC should be a center for joint operational planning and joint intelligence; staffed by personnel for the various agencies . . . The head of the NCTC should be appointed by the president, and should be equivalent in rank to a deputy head of a cabinet department . . . report[ing] to the national

priority is to direct a concerted effort among all the government intelligence agencies.[156]

These goals were partially accomplished in March 2004 when the Office of Terrorism and Financial Intelligence was created. However, the 9/11 Commission cites six problems that indicate a continued need to restructure the intelligence community. National intelligence, the Commission complains, is still organized around the agencies, creating structural barriers to a performing joint intelligence work.[157] The intelligence community should have the ability to pool [at all times] information gathered abroad with information gathered domestically, using a common method of collection, processing, reporting, sharing and analyzing.[158] Another suggestion would be to find a more efficient way to examine and analyze the data collected in SARs and CTRs, so relevant information could be used in a timely manner to protect Americans. The United States government has spent over $300 *billion* dollars[159] on fighting terrorism since 2001, and, by the government's own estimates, has recovered only $61.5 million dollars through the use of the BSA created SAR[160] reporting device.

> intelligence director, an office whose creation [the Commission also recommends], placed in the Executive Office of the President ... [thereby] indirectly [reporting] to the President.

156. Few realize how vast the United States intelligence community is. Currently there is an Office of the Director of Central Intelligence, which included the Office of the Deputy Director of Central Intelligence for Community Management, the Community Management Staff, the Terrorism Threat Integration Center, the National Intelligence Council, and other community offices. The Central Intelligence Agency (CIA), which performs human source collection, all-source analysis, and advanced science and technology. The National Intelligence Agencies: National Security Agency (NSA), which performs signals collection and analysis, National Geospatial-Intelligence Agency (NGA), which performs imagery collection and analysis, the National Reconnaissance Office (NRO), which develops, acquires, and launches space systems for intelligence collection, and other national reconnaissance programs. Departmental intelligence agencies [consists of]: Defense Intelligence Agency (DIA) of the Department of Defense, Intelligence entities of the Army, Navy, Air Force, and Marines, Bureau of Intelligence and Research (INR) of the Department of State, Office of Terrorism and Finance Intelligence of the Department of Treasury, Office of Intelligence and the Counterterrorism and Counterintelligence Divisions of the Federal Bureau of Investigation of the Department of Justice, Office of Intelligence of the Department of Energy, Directorate of Information Analysis and Infrastructure Protection (IAIP) and Directorate of Coast Guard Intelligence of the Department of Homeland Security. *Id.* at 407–408.

157. *See* THE 9/11 COMMISSION REPORT, *supra* note 136, at 408.

158. *Id.* at 409

159. *House Passes Iraq Spending Bill*, ASSOC. PRESS, May 5, 2005, *available at* http://www.cbsnews.com/stories/2005/05/04/politics/main692881.shtml?CMP=ILC-SearchStories .

160. *See* Julie Wakefield, *Following the Money*, GOV'T EXECUTIVE MAG., Oct. 1, 2000, *available at* http://www.govexec.com/features/1000/1000s5.html (finding that the FBI

AI[161] is not working. Each and every Comment letter received by FinCEN, and many other governmental agencies and committees, from members of the banking community, bank executives, and industry analysts *begs* the government to clearly define the requirements to file a SAR or CTR. Other alternatives would be to eliminate the identity verification requirements or at least reduce them, reduce the requirements to notify the financial institutions Board of Directors and committees of the Board, reduce the filing requirements or at least the CTR reporting threshold, more clearly define the "structuring" reporting perimeters, or give additional guidance on filing SARs concerning continuing activity of a similar nature by the same customer. The repeated cry is to reduce or eliminate redundant, inefficient, and unnecessary aspects of the regulatory compliance burden. This inefficiency and its associated cost is passed on in increased fees to bank customers, and perhaps even reduced pay for bank employees.

More importantly, the discretion to file or not to file a SAR or CTR must *not* be any longer only left in the hands of tellers. Despite the probable increase in labor hours of those more qualified to make these decisions, this proposal would allow bank tellers to continue making initial reports. These reports would then be relayed to an internal central clearing house in each bank— monitored by bank personnel astute and educated in the BSA—and would only be allowed to continue on to the SARS system if, after full and fair analysis, the possibility of terrorism or money laundering is clearly identified. In addition, the Department of the Treasury simply must act to promulgate less burdensome and more specific SAR and CTR filing rules for banks to follow.

To work further towards a solution, Americans should concern themselves with securing United States Supreme Court review of the Constitutionality of the Patriot Act's effect on rights like the Fourth Amendment. Shall we as a country abandon or reaffirm the First and Fourth Amendments to the U.S. Constitution? For 200 years, the Supreme Court has been the protector of our legal rights. and must now create a right for Americans to be free from unreasonable searches and seizures *in their bank accounts*. Beginning with *Connally,* the Court has taken a wrong turn on the Fourth Amendment issue. Justice Douglas' criticism of the reporting provisions of the BSA makes the point that:

> [t]hese omnibus grants of power allow the Executive Branch to make the law as it chooses in violation of the teachings . . . that lawmaking is a congressional, not an Executive function . . . The Fourth Amendment warrant requirements may be removed by constitutional amendment but they certainly cannot

---

uses SARs in 98 percent of its bank fraud cases and has recovered $61.5 million dollars in defrauded monies with the reports).

161. *See supra* note 70.

> be replaced by the Secretary of the Treasury's finding that certain information will be highly useful in "criminal, tax, or regulatory investigations or proceedings."[162]

A search and seizure conducted without a warrant is *per se* unreasonable, subject to "'jealously and carefully drawn' exceptions."[163] "One's bank accounts are within the 'expectations of privacy' category . . . However, the historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[164]

The End Racial Profiling Act must be enacted. Yes, for the Act's various articulated reasons, but also for one of its most vital canons—to establish a cause of action for victims of intelligence gathering abuses. Civil litigation and criminal actions concerning racial profiling incidents have been notoriously difficult to prosecute. If there are no effective checks and balances, Constitutional infringements on American citizens remain unbridled and abuses of power continue unabated, leaving victims of racial profiling with even less protection.

The U.S. House of Representatives is moving forward along a path parallel to ERPA. The first federal profiling legislation passed the House and is awaiting Senate approval. And then of course, there remains the question of whether President Bush will veto the entire bill. The Congressional Black Caucus endorsed the Transportation Equity Act: A Legacy for Users, sponsored by Delegate Eleanor Holmes Norton, as part of a $275 billion transportation bill which provides $60 million over six years requiring states to develop proactive anti-profiling measures and document racial statistics on traffic stops. Holmes has characterized the bill as a back-door attempt, as opposed to the front-door anti-police mandatory civil rights profiling law that Representative John Conyers has been trying to get through for the last two sessions of Congress.[165] Clearly something must be done. Racial profiling is a civil rights issue that will not disappear without the proper attention. For too long this issue has plagued African Americans; and now Muslims, Arab Americans, Middle Easterners, and even those who "look Middle Eastern" are being subjected to equally poor and unfair treatment. Too many victims of profiling have died on the nation's highways or been refused redress in the courts for the ill-advised behavior of police officers. We cannot stand by as racial profiling continues to be projected into the terrorism melee. America maintains it is a nation governed by constitutional pro-action. If that is

---

162. *Schultz*, 416 U.S. at 90–91 .

163. *Id.* at 89.

164. *Id.*

165. End Racial Profiling Act, H.R. 3847, 108th. Cong. (2004); Transportation Equity Act: A Legacy for Users, H.R. 3550, 108th Cong. (2003).

true, the rights of all Americans must be protected. H.R.3550 is a sound first step on the journey to constitutional equality.

Cries of the Office of Homeland Security seem to now legitimize group based profiling, contravening constitutional rights and individual dignity. Fighting the "War on Terror" and safeguarding our financial systems is estimated to cost taxpayers $250.9 million for fiscal year 2005.[166] In 2005, there were close to twelve million filings of CTRs and SARs,[167] an overwhelming majority of which contain information largely irrelevant to combat terrorism and will likely not be examined by treasury officials for months after they are filed. The very creation of Patriot Act I and the impending Patriot Act II contribute to the enormous pallor and wickedness of racial profiling throughout our country, and in banks. All of this a response to what the 9/11 report says was approximately $400,000 to $500,000 in terrorist dollars which did not really pass through our banks.[168]

The body of federal legislation passed in response to infringements on American rights to privacy in their bank accounts, is a radical indication of how important this issue is to all facets of American ethnicity. Considering how important this is, the Supreme Court should at the very least re-hear this matter and re-examine the need to extend Fourth Amendment protection to financial matters. We cannot and must not sort the contents of the American melting pot while dramatically undermining the melting-pot ideal, as we have historically done to African Americans. Being an American means enjoying the rights of an American.

166. *The Budget Overview for the Department of the Treasury: Hearing Before the Subcomm. on Transportation, Treasury, and General Government of the S. Comm. on Appropriations*, 108th Cong. (2004) (statement of John Snow, Treasury Secretary of the United States), *available at* http://appropriations.senate.gov/hearmarkups/record.cfm?id=220599 .

167. *Statement of Stanley E. Morris, supra* note 70, at 114 (testifying that depository institutions filed 297,753 SARs prior to October 28, 2004, and projecting that number to double in 2005). *See also* Government Appropriations for 1998, Testimony of Stanley E. Morris, Director Financial Crimes Enforcement Network, Tuesday March 4, 1997, p.114. Morris testified that 11 million CTRs are filed each year.

168. THE 9/11 COMMISSION REPORT, *supra* note 136, at 169–72.